奠基
计算机网络

韩立刚　李文斌　潘刚柱　张庆力　**编著**

清华大学出版社

北 京

内 容 简 介

本书是一本讲解计算机网络基础的图书，但其内容并没有局限于计算机网络，还包括了网络安全、搭建网络服务器等实用操作内容。本书一改传统计算机网络教材艰涩的叙述方式，而是基于笔者多年的网络运营经验从实用角度阐述理论，希望可以给读者不一样的阅读体验。本书使用 Packet Tracer 和 Dynamips 两款路由器模拟软件为读者搭建好逼真实验环境，为您的学习扫除障碍。

本书涉及的内容，理论部分包括网络设备、开放式系统互联（OSI）、IP 地址、TCP/IP 协议、安装服务器、配置服务器网络安全、灰鸽子木马防治、P2P 终结者的工作原理。路由器操作部分包括网络操作系统（IOS）的配置。路由部分包括静态路由、路由汇总、默认路由。动态路由讲述了 RIP、EIGRP 和 OSPF。交换部分包括交换机端口安全和 VLAN 管理。网络安全包括标准访问控制列表、扩展访问控制列表。网络地址转换包括静态 NAT 和动态 NAT 及端口地址转换。IPv6 包括 IPv6 地址、IPv6 的动态和静态路由、IPv6 和 IPv4 共存技术。广域网包括广域网封装 PPP、HDLC 和帧中继、路由器和 Windows 实现的 VPN。

本书光盘包含 30 小时的计算机网络相关视频操作以及 PPT 教学课件。

本书适合于作为计算机网络自学教材、大专院校教材、社会培训教材、CCNA 教辅等。另外，本书提供的一些实用网络操作，对网络从业人员也具有相当的参考价值。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

奠基——计算机网络 / 韩立刚等编著. —北京：清华大学出版社，2011.10

ISBN 978-7-302-25515-4

Ⅰ.①奠… Ⅱ. ①韩… Ⅲ. ①计算机网络——基本知识 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2011）第 087948 号

责任编辑：栾大成
装帧设计：
责任校对：徐俊伟
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：188×260　　**印　张**：27.5　　**字　数**：690　千字
附 DVD 1 张
版　　次：2011 年 10 月第 1 版　　**印　次**：2011 年 10 月第 1 次印刷
印　　数：1～5000
定　　价：59.00 元

产品编号：042602-01

前　言

“奠基计算机网络”是一本讲解计算机网络基础的图书，但其内容并没有只局限于计算机网络，还包括网络安全、网络排错、Windows Server 2003 搭建网络服务器和使用 Windows 实现的网络功能。

该书主要面向当前和未来的网络技术，因此没有过多地介绍互联网的历史，而是对下一代网络协议 IPv6 进行了详尽的介绍。该书没有打算让读者去研发 TCP/IP 协议，因此对于 TCP/IP 封装起来的内部的工作机制没有过多的讲解，但通过在 Windows Server 2003 上安装服务和配置服务器安全，使读者能够更深入地理解 TCP/IP 协议传输层和应用层协议之间的关系、服务和端口的关系、端口和网络安全的关系。学习后，你将能够通过查看建立的 TCP 会话来检查 Windows 操作系统是否中了木马，并使用 IPSec 防止木马。该书没有打算让读者去制造网卡或其他网络设备，因此没有为你详细讲述网卡传输信号的细节，也不会让你用复杂的公式计算以太网数据包传输延迟，但对于网络中使用网卡 MAC 地址欺骗造成的网络故障进行了详尽的讲解，为你展示了使用捕包工具捕获数据包排除网络故障的方法。本书没有打算让读者去改进动态路由的算法，因此对于复杂的动态协议的算法没有过多的讲解，但对于各种动态路由协议的适用场景和特点进行了详细的介绍和比较，并设计实验环境供你体验。总之，本书为你提供了对所学知识操作一遍的机会，消除读者对纯理论的神秘感，所有的实验环境在光盘中都为你提供了。

为什么写这本书

对于立志于投身网络的青年人，选对教材是非常重要的。一个初学网络的人，如果选择了理论性很强的书作为入门读物将会是一个悲剧。这类专业网络图书套路相近：网络技术，计算机网络发展史，深不可测的路由算法，计算以太网数据帧的延迟，对称加密的算法和非对称加密算法，HTTP 协议……，对这些内容进行无懈可击的阐述，你只要背过了这些定义，考个高分没问题。这类专著学下来，你会觉得道理上明白了，但是对于解决具体实际的问题，你还是束手无策。这样的书学完，你能使用捕包工具解决网络拥塞的问题吗？你能通过所学的 TCP/IP 知识配置安全的服务器吗？你能使用 IPSec 严格控制服务器的流量吗？你能通过所学知识查找木马活动吗？给你一个路由器你能够配置路由表吗？……

我们并不是说市场上一些网络图书内容不好，只是说，可能它们并不适合实践，而更适合应付考试或者理论研究。

《奠基——计算机网络》，是针对有志进入企业 IT 部门的学生或者从业者编写的，所有理论都和实际问题相关联。对那些在工作中没有指导意义的理论进行了精简，而对于工作中可能遇到的问题增加了篇幅，同时增加了大量案例实验，让网络学习变得有趣。

高校的计算机网络教程大多偏重理论，没有针对具体的网络设备安排课程内容。如果报考研究生，掌握这些理论是必不可少的。本书中的案例也可作为高校计算机网络的实验手册，这对于你深刻理解计算机网络中的理论有很大帮助。

再就是针对 Cisco 网络工程师认证的教程《CCNA 学习指南》，是针对 Cisco 认证的教材。其内容只局限于网络知识和 Cisco 路由器的操作，没有进一步扩展，比如讲授 TCP/IP，没有更进一步地讲述网络安全，也没有讲述在 Windows 操作系统上实现的网络安全。再比如，在讲授网络地址转换 NAT 时，只讲到在 Cisco 路由器上实现的地址转换，并没有讲述在 Windows Server 上实现的 NAT。在讲授 Cisco 路由器实现的 VPN 时，没有讲述使用 Windows 实现的 VPN。在讲授 IPv6 时，没有讲授 IPv4 和 IPv6 共存技术的具体实施。

本人从事 IT 技术培训工作十余年，并多年从事微软的产品技术支持服务，在排除操作系统和网络故障方面积累了大量的经验。在讲授 CCNA 课程时，将为客户排除网络故障的大量案例插入合适的章节，使抽象的理论和实际结合，在授课过程中尽量避免使用听起来高深的术语，而是使用直白流畅的语言进行阐述。经过多年的积累沉淀，逐渐形成自己 CCNA 授课的风格和内容，广受学员欢迎，尤其是初学网络的学员。

对于自学计算机网络的学生，苦于没有网络设备，使得网络的学习仅停留于理论，而陷入困顿。有些学校即便有网络设备，也很难为每一个学员提供实验所需的网络环境。基于此，本书使用 Packet Tracer 和 Dynamips 软件为读者设计、搭建好了实验环境，读者只需打开软件，按着书上的步骤验证所需知识即可。

本书适合谁

- 计算机网络的初学者
- 高校在校生
- 企业 IT 员工

另外，如果你打算报考计算机方向的研究生，这本书并不适合你；如果你打算学完之后从事网络方面的工作，本书是最佳选择。

对读者的要求

要求读者有使用网络的经验，那怕你会 QQ 聊天或网络偷菜，也就算是有了学习本书的基础。

本书特色

- 侧重应用，尽量挖掘理论在实践中的应用。
- 使用路由器模拟软件 Packet Tracer 设计实验和实验步骤。
- Dynamips 软件搭建实验环境。有些实验 Packet Tracer 不支持，就使用 Dynamips 软件模拟真实的路由操作系统。
- 针对理论设计了实验环境，帮助你理解理论。
- 有和教材相对应的 PPT，适合作为学校教材。
- 光盘中教学有视频，帮助你自学。
- 光盘中的虚拟机包括所有的实验环境，开机即可使用。
- 学习本书，你只需一台内存在 1GB 以上的计算机即可。

本书主要内容

第 1 章：介绍了局域网、广域网、服务器、客户机、OSI 参考模型、网络设备等基本概念；集线器、交换机、路由器的功能；网卡、网线、直通线、交叉线、全反线的应用场景；OSI 参考模型与网络排错以及网络安全的关系；Cisco 组网的三层模型。

第 2 章：详细阐述 TCP/IP 的层次结构，以及每层包含的协议，讲解了传输层两个协议——TCP 和 UDP 的应用场景，应用层协议和传输层协议的关系，应用层协议和服务之间的关系；演示了在 Windows Server 2003 上安装配置 FTP 服务、Web 服务、POP3 服务、SMTP 服务和 DNS 服务，启用服务器的远程桌面，并且配置客户端连接这些服务器；配置 Windows 防火墙保护 Windows XP 安全和使用 TCP/IP 筛选配置服务器安全，防止主动入侵计算机；配置 IPSec 严格控制进出服务器的数据流量，避免木马程序造成威胁；展示使用捕包工具排除网络故障。

第 3 章：本章内容包括 IP 地址层次结构、IP 地址分类、保留的 IP 地址、私有地址、等长子网划分和变长子网划分。

第 4 章：讲述如何使用 Dynamips 软件在计算机上运行路由器 IOS，并搭建本书的实验环境，然后在这个软件上运行 IOS 进行路由器的常规配置来熟悉 Cisco 命令行界面；当完全熟悉了这个界面后，你将能够配置主机名、口令和其他更多的内容，并且通过使用 Cisco IOS 来进行排错；使用安全设备管理器（SDM）管理路由器、恢复路由器密码、升级和安装路由器 IOS。

第 5 章：在本章中您将学习数据包路由的详细过程，以及网络能畅通的必要条件。通过本章的学习，您将能够排除数据包路由产生的网络故障，并且能够使用路由汇总和默认路由简化路由表的配置，你还能够在 Windows 中配置路由和默认路由。通过配置路由器的路由表，可以实现网络的负载均衡。

第 6 章：本章讲述配置路由器使用动态路由协议自动构建路由表；讲述 RIP（路由信息协议）、EIGRP（增强内部网关路由协议）以及 OSPF（开放式最短路径优先）的工作特点和配置方法；配置 RIP 和 EIGRP 支持变长子网和不连续子网，配置 EIGRP 进行手动汇总，配置 OSPF 协议多区域，在边界路由器进行汇总；配置路由再发布、将静态路由发布到动态路由、不同动态路由协议之间实现路由再发布。

第 7 章：本章介绍交换机、集线器和网桥设备的区别，以及交换机如何优化网络；介绍设计高可用的交换网络和交换机阻断环路的生成树技术；交换机端口安全；介绍什么是 VLAN（虚拟局域网）、如何创建 VLAN，以及将相应的接口指定到特定的 VLAN，配置干道链路和 VLAN 间路由；使用 VTP（VLAN 间干道协议）协议简化 VLAN 管理。

第 8 章：本章内容包括从 OSI 参考模型来看网络安全，典型的安全网络架构，安全威胁，标准访问控制列表，扩展访问控制列表，使用访问控制列保护路由器安全，基于时间的访问控制列表，使用 ACL 降低安全威胁。

第 9 章：本章介绍网络地址转换（Network Address Translation，NAT）、动态网络地址转换和端口地址转换（Port Address Translation，PAT），PAT 也称为网络地址转换复用；介绍 NAT、PAT 和端口映射的应用场景以及配置方法；演示了使用 Windows XP 配置连接共享实现 NAT 和端口映射、在 Windows Server 2003 上配置 NAT 和端口映射。

第 10 章：本章介绍 IPv6 相较现在的 IP 有哪些方面的改进，IPv6 的地址体系，IPv6 下的计算机地址配置方式，IPv6 的静态路由和动态路由，支持 IPv6 的动态路由协议 RIPng、EIGRPv6 和 OSPF 协议 v3 的配置；IPv6 和 IPv4 共存技术、双协议栈技术、6 to 4 的隧道技术、ISATAP 隧道和 NAT-PT 技术。

第 11 章：本章主要为大家介绍广域网使用的协议，重点讲授广域网协议 HDLC、PPP 和帧中继。同时还会介绍 VPN 的配置，使用 Cisco 路由器和 Windows Server 2003 配置为远程访问服务器。

致 谢

河北师范大学软件学院采用“校企合作”的办学模式。在课程体系设计上与市场接轨；在教师的使用上，大量聘用来自企业一线的工程师；在教材及实验手册建设上，结合国内优秀教材的知识体系，大胆创新，开发了一系列理论与实践相结合的教材（本教材即是其中一本）。在学院新颖模式的培养下，百余名学生进入知名企业实习或已签订就业合同，得到了用人企业的广泛认可。这些改革及成果的取得，首先要感谢河北师范大学校长蒋春澜教授的大力支持和鼓励，同时还要感谢河北师范大学校党委对这一办学模式的肯定与关心。

在本书整理完成的过程中，对河北师范大学数信学院院长邓明立教授、软件学院副院长赵书良教授以及李文斌副教授表示真诚的谢意，是他们为本书的写作提供了一个良好的环境，是他们为本书内容的教学实践保驾护航。他们与编著者关于教学的沟通与交流为本书提供了丰富的案例和建议。感谢河北师范大学软件学院教学团队中的每一位成员，还要感谢河北师范大学软件学院每一位学生，是他们的友好、热情、帮助和关心促使本书的形成。

最后，感谢我的家人在本书创作过程中给予的支持与理解。

韩立刚

MSN：onesthan@hotmail.com

QQ：458717185

目　录

第 1 章　计算机网络 1
1.1　局域网和广域网 2
1.2　服务器和客户机 3
1.3　网际互联模型 4
1.3.1　分层的方法 4
1.3.2　参考模型的优点 5
1.3.3　OSI 的分组 7
1.4　理解 OSI 参考模型 7
1.4.1　实例：应用程序包含 IP 地址带来的麻烦 7
1.4.2　OSI 参考模型与排错 8
1.4.3　通过建立的会话查看木马 . 11
1.5　网络设备 13
1.5.1　网卡 13
1.5.2　网线 17
1.5.3　集线器 19
1.5.4　交换机 20
1.5.5　路由器 21
1.6　数据封装 22
1.7　传输模式 24
1.7.1　半双工和全双工以太网 24
1.7.2　设置网卡的双工模式 25
1.8　Cisco 组网三层模型 27
1.8.1　核心层 28
1.8.2　汇聚层 28
1.8.3　接入层 29
1.8.4　高可用网络设计 29
1.9　习题 30
第 2 章　TCP/IP 协议 33
2.1　OSI 和 DoD 模型 34
2.2　传输层协议 34
2.2.1　传输控制协议 35
2.2.2　用户数据报协议 35
2.3　应用层协议 36
2.3.1　应用层协议和传输层协议的关系 36
2.3.2　应用层协议和服务的关系 . 37
2.3.3　示例 1：查看远程桌面侦听的端口 38
2.3.4　示例 2：端口冲突造成服务启动失败 40
2.4　应用层协议和服务 41
2.4.1　在 Windows Server 2003 上安装服务 42
2.4.2　配置 FTP 服务器 45
2.4.3　配置 Web 服务器 48
2.4.4　配置 SMTP 服务和 POP3 服务 51
2.4.5　启用远程桌面且更改默认端口 59
2.4.6　配置 DNS 服务器 62
2.5　配置服务器网络安全 66
2.5.1　端口扫描 67
2.5.2　使用 Telnet 排除网络故障 67
2.5.3　Windows 防火墙保护客户端安全 69
2.5.4　使用 TCP/IP 筛选保护服务器安全 73
2.5.5　使用 IPSec 保护服务器安全 78
2.6　网络层协议 89
2.6.1　IP 协议 89
2.6.2　ICMP 协议 93
2.6.3　IGMP 协议 98
2.6.4　ARP 协议 98
2.7　使用捕包工具排除网络故障 104
2.7.1　示例：查看谁在发送广播包 104
2.7.2　捕包软件安装的位置 106
2.8　习题 108
第 3 章　IP 地址 113
3.1　理解 IP 地址 114

3.1.1 IP 术语 114
3.1.2 IP 层次结构 114
3.1.3 网络地址 115
3.2 IP 地址分类 116
3.2.1 A 类地址 116
3.2.2 B 类地址 118
3.2.3 C 类地址 119
3.2.4 D 类和 E 类地址 120
3.2.5 保留的 IP 地址 120
3.2.6 私有 IP 地址 122
3.3 等长子网划分 123
3.3.1 子网划分预备知识 123
3.3.2 子网掩码的作用 124
3.3.3 CIDR 124
3.3.4 等长子网划分 125
3.3.5 判断 IP 地址所属的网段 . 129
3.3.6 A 类网络子网划分 130
3.4 变长子网划分 131
3.4.1 示例：变长子网划分 131
3.4.2 超网 133
3.4.3 合并网络的规律 134
3.5 习题 135
第 4 章 Cisco IOS 141
4.1 Cisco 路由器的硬件和 IOS 142
4.1.1 Cisco 路由器的硬件分类. 142
4.1.2 Cisco 路由器的主要组件. 144
4.1.3 路由器 IOS 命名 145
4.2 路由器模拟软件 146
4.2.1 Packet Tracer 146
4.2.2 Dynamips 147
4.3 连接到路由器进行配置 147
4.3.1 使用超级终端配置路由器148
4.3.2 使用超级终端 Telnet 路由器 150
4.4 路由器的常规配置 151
4.4.1 实验环境和要求 151
4.4.2 使用 Dynamips 搭建实验环境 152
4.4.3 查看路由器信息 156
4.4.4 配置路由器的全局参数... 157
4.4.5 配置路由器的接口 158
4.4.6 配置路由器允许通过 Telnet 配置 161
4.4.7 查看、保存和删除路由器配置 163
4.4.8 加密口令 164
4.5 Cisco 命令行帮助功能 164
4.5.1 使用帮助功能和命令简写165
4.5.2 使用 do 命令 166
4.6 Cisco 安全设备管理器 166
4.7 重设路由器密码 169
4.8 安装和升级路由器 IOS 170
4.8.1 备份路由器的 IOS 170
4.8.2 安装或升级路由器 IOS ... 171
4.9 配置路由器名称解析 173
4.9.1 建立主机列表 173
4.9.2 配置 DNS 进行域名解析 173
4.10 使用 Cisco 发现协议 174
4.10.1 获取 CDP 定时器和保持时间信息 174
4.10.2 收集邻居信息和显示 CDP 状态 175
4.11 路由器 Telnet 路由器 177
4.12 习题 178
第 5 章 静态路由 181
5.1 IP 路由 182
5.1.1 配置静态路由 183
5.1.2 删除静态路由 186
5.2 路由汇总 188
5.2.1 通过路由汇总简化路由表188
5.2.2 路由汇总例外 189
5.2.3 无类域间路由（CIDR）. 190
5.3 默认路由 190
5.3.1 使用默认路由作为指向 Internet 的路由 191
5.3.2 让默认路由代替大多数网段的路由 192
5.3.3 使用默认路由和路由汇总

简化路由表..... 193
5.3.4 Windows 上的默认路由和网关..... 194
5.4 网络负载均衡..... 197
5.4.1 配置和验证网络负载均衡..... 197
5.4.2 另外一种网络负载均衡... 200
5.4.3 热备份路由协议（HSRP）..... 201
5.5 总结..... 202
5.6 实验..... 203
5.6.1 试验 1：静态路由..... 203
5.6.2 实验 2：使用默认路由.... 206
5.6.3 实验 3：使用默认路由和路由汇总..... 207
5.6.4 实验 4：网络排错..... 209
5.7 习题..... 210
第 6 章 动态路由..... 213
6.1 动态路由..... 214
6.2 RIP 协议..... 215
6.2.1 RIP 的配置过程..... 215
6.2.2 RIPv1 和 RIPv2 220
6.3 EIGRP 协议 222
6.3.1 EIGRP 的配置过程 223
6.3.2 关闭 EIGRP 的自动汇总 . 225
6.3.3 查看 EIGRP 的配置和路由表 225
6.3.4 EIGRP 手动汇总 225
6.3.5 确认 EIGRP 选择的最佳路径..... 226
6.3.6 查看 EIGRP 的备用路径 . 227
6.3.7 查看 EIGRP 邻居 228
6.3.8 显示 EIGRP 协议活动 228
6.3.9 更改 EIGRP 的默认设置 . 229
6.4 OSPF 协议 229
6.4.1 OSPF 相关术语 230
6.4.2 支持多区域..... 231
6.4.3 OSPF 的 network 参数 233
6.4.4 配置 OSPF 单区域 234
6.4.5 检查路由表..... 235
6.4.6 查看 OSPF 链路状态数据库 236
6.4.7 测试 OSPF 收敛速度..... 236
6.4.8 OSPF 多区域..... 238
6.4.9 OSPF 路由汇总 240
6.5 RIP、EIGRP 和 OSPF 协议的对比..... 241
6.5.1 路由协议的类型..... 241
6.5.2 路由协议的优先级..... 242
6.5.3 验证路由协议的优先级... 243
6.6 路由再发布..... 245
6.6.1 将静态路由发布到动态路由 246
6.6.2 RIP 和 EIGRP 路由再发布 248
6.6.3 OSPF 和 EIGRP 路由再发布 251
6.7 实验..... 253
6.7.1 实验 1：配置 RIPv2 支持变长子网 253
6.7.2 实验 2：配置 RIPv2 支持不连续子网 254
6.7.3 实验 3：配置 EIGRP 手动汇总 255
6.7.4 实验 4：OSPF 排错 258
6.8 习题..... 258
第 7 章 交换 261
7.1 局域网组网设备..... 262
7.1.1 集线器..... 262
7.1.2 网桥..... 262
7.1.3 交换机..... 263
7.1.4 查看交换机的 MAC 地址表 264
7.1.5 交换机上配置监控端口... 265
7.2 生成树协议..... 266
7.2.1 生成树协议..... 267
7.2.2 生成树术语..... 267
7.2.3 生成树的操作..... 268

7.2.4 生成树的端口状态 269
7.2.5 确认和更改根桥 270
7.2.6 关闭 VLAN 1 的生成树 ... 272
7.3 优化生成树 272
7.3.1 生成树快速端口 272
7.3.2 生成树上行链路快速 273
7.3.3 启用快速生成树协议（RSTP）802.1w 274
7.4 交换机端口安全 274
7.4.1 端口和 MAC 地址绑定 274
7.4.2 控制端口连接计算机的数量 276
7.5 VLAN 277
7.5.1 什么是 VLAN 278
7.5.2 创建和管理 VLAN 279
7.5.3 跨交换机的 VLAN 281
7.5.4 配置干道链路 283
7.5.5 帧标记 285
7.5.6 VLAN 干道协议（VTP） 286
7.5.7 配置 VTP 域 287
7.6 配置 VLAN 间路由 289
7.6.1 单臂路由器实现 VLAN 间路由 289
7.6.2 多层交换机实现 VLAN 间路由 291
7.7 交换机 EtherChannel 292
7.8 习题 295
第 8 章 网络安全 299
8.1 网络安全简介 300
8.1.1 从 OSI 参考模型来看网络安全 300
8.1.2 典型的安全网络架构 301
8.1.3 防火墙的种类 302
8.1.4 常见的安全威胁 303
8.2 访问控制列表 305
8.2.1 标准访问控制列表 306
8.2.2 扩展访问控制列表 309
8.2.3 使用访问控制列表保护路由器 311
8.3 基于时间的访问控制列表 312
8.3.1 查看和设置路由器的时间 312
8.3.2 定义时间段 313
8.3.3 在访问控制列表中使用时间 313
8.4 使用访问控制列表降低安全威胁 314
8.4.1 IP 地址欺骗对策 315
8.4.2 DoS TCP SYN 攻击对策 . 316
8.4.3 DoS Smurf 攻击对策 317
8.4.4 过滤 ICMP 消息 318
8.4.5 DDoS 对策 319
8.5 访问控制列表的位置 320
8.6 习题 321
第 9 章 网络地址转换 325
9.1 网络地址转换技术简介 326
9.1.1 NAT 的应用场景 326
9.1.2 NAT 的类型 326
9.2 实现网络地址转换 327
9.2.1 配置静态 NAT 327
9.2.2 配置动态 NAT 329
9.2.3 配置 PAT 332
9.2.4 配置端口映射 333
9.3 在 Windows 上实现网络地址转换和端口映射 336
9.3.1 在 Windows XP 上配置连接共享和端口映射 336
9.3.2 在 Windows Server 2003 上配置网络地址转换和端口映射 338
9.4 实验 342
9.5 习题 343
第 10 章 IPv6 347
10.1 为什么需要 IPv6 348
10.1.1 IPv4 的不足之处 348
10.1.2 IPv6 的改进 349
10.1.3 IPv6 协议栈 350
10.1.4 ICMPv6 协议的功能 351

10.2 IPv6 寻址 353
10.2.1 IPv6 寻址及表达式 354
10.2.2 IPv6 的地址类型 355
10.2.3 IPv6 中特殊的地址 356
10.2.4 IPv6 计算机地址配置方法 356
10.3 配置 IPv6 路由 361
10.3.1 配置 IPv6 静态路由 362
10.3.2 配置 RIPng 支持 IPv6 363
10.3.3 配置 EIGRPv6 支持 IPv6 365
10.3.4 配置 OSPFv3 支持 IPv6 368
10.4 IPv6 和 IPv4 共存 370
10.4.1 双协议栈技术 371
10.4.2 6 to 4 隧道技术 372
10.4.3 ISATAP 隧道 374
10.4.4 NAT-PT 379
10.5 习题 384
第 11 章 广域网 387
11.1 广域网简介 388
11.1.1 广域网术语 388
11.1.2 广域网连接类型 389
11.1.3 通用的广域网协议 390
11.2 典型的广域网协议 391
11.2.1 HDLC 391
11.2.2 点到点 PPP 393
11.2.3 帧中继 398
11.3 虚拟专用网 407
11.3.1 VPN 使用的广域网协议 409
11.3.2 配置路由器为 VPN 服务器 409
11.3.3 配置 Windows 服务器为 VPN 服务器 417
11.4 习题 425

第 1 章　计算机网络

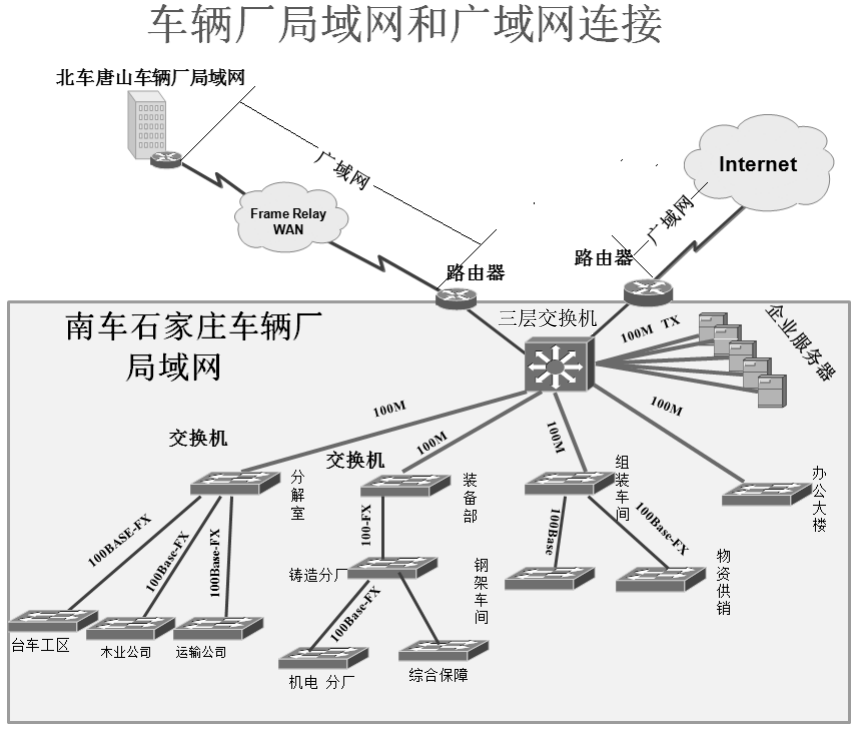
本章介绍了局域网、广域网、服务器、客户机、OSI 参考模型、网络设备等基本概念；集线器、交换机、路由器的功能；网卡、网线、直通线、交叉线、全反线的应用场景；OSI 参考模型与网络排错以及网络安全的关系；Cisco 组网的三层模型。

本章主要内容：

- 局域网和广域网
- 服务器和客户机
- OSI 参考模型
- OSI 参考模型对网络排错的指导
- OSI 参考模型与网络安全
- 网络设备
- 数据封装
- 全双工和半双工以太网
- Cisco 组网三层模型

1.1 局域网和广域网

在讲解网络理论之前，先看看石家庄车辆厂的网络拓扑。石家庄车辆厂分为南车石家庄车辆厂和北车唐山车辆厂，都有自己的局域网，而访问 Internet 的出口在南车石家庄车辆厂，如图 1-1 所示。



▲图 1-1　车辆厂网络拓扑图

南车和北车分别位于石家庄市和唐山市，该公司不可能自己布线将两个城市的局域网连接起来，因此租用网通的帧中继连接，其租用的带宽为 2M。

现在企业局域网使用的设备主要是交换机和三层交换机，三层交换机实现企业 VLAN 间的路由。局域网的带宽为 10M、100M 和 1000M 几个标准。

路由器用来连接广域网，因为路由器有广域网接口，可以和网通或电信的广域网线路连接。

结合以上实例来理解一下局域网和广域网及其区别。

- 局域网一般企业自己购买设备，将物理位置较近办公区的计算机使用网络设备连接起来，一般覆盖范围是几千米以内。局域网使用的网络设备有集线器或交换机，带宽为 10M、100M 和 1000M 这几个标准，而使用无线连接的局域网带宽标准则为 54M。
- 广域网一般企业租用网通或电信的线路，通常跨接的范围从几十公里到几千公里，它能连接多个城市或国家。广域网的带宽由企业所付的费用决定，比如我们上网的 ADSL 就是租用网通或电信的服务，带宽有 1M、2M 和 4M 几个标准。

广域网和局域网的划分有时候也不是单纯从距离上划分的。比如你和邻居都分别使用 ADSL 访问 Internet，当你访问邻居的计算机共享文件或其他资源的时候，你的计算机和邻居的计算机就是广域网连接，因为你们是通过用租网通或电信提供的服务连接的。如果你和邻居的计算机使用网线直接连接，则是局域网连接。

再比如一个企业的两栋大楼距离几公里，这两栋大楼中的局域网通过公司自己部署光纤连接，我们也可以将其理解为局域网，因为没有租用网通或电信提供的服务。

1.2 服务器和客户机

现在介绍服务器和客户机的区别。

在网络和数据库的相关图书中，服务器和客户机是两个经常出现的术语。它们的含义从不同的角度来理解是不一样的，初学者容易在这些术语上产生困惑。

1. 从硬件角度来理解

硬件角度（物理角度）的客户机通常指一些适合家庭或办公环境使用的笔记本电脑（见图 1-2）或台式机（见图 1-3）。这些计算机上网的目的是享受各种网络服务，如电子邮件服务、网站浏览服务等。



▲图 1-2　笔记本电脑



▲图 1-3　台式机

硬件角度的服务器是指一些有别于普通用户使用的 PC 的特殊计算机，如图 1-4 所示，这些计算机在网络中用来提供各种网络服务。为了适应大容量的数据存储和频繁的客户机访问操作，这些计算机一般都配备可热插拔的、大容量的硬盘，24 小时不间断的 UPS 电源等硬件设备。



▲图 1-4　刀片服务器

2. 从软件角度来理解

软件角度（逻辑角度）的客户机（Client）通常指一些安装了享受网络服务软件的计算机。比如，我们上网浏览网站需要 IE 浏览器，这里的 IE 浏览器就是一种 Web 客户机软件，我们就称安装了 IE 浏览器的计算机是一台 Web 客户机；再如，我们使用电子邮件服务就需要用 Outlook 或者 Foxmail，我们就称安装了电子邮件软件的计算机是一台 E-mail 客户机。

问题	我的计算机上同时安装有电子邮件软件和 IE 浏览器，那么可不可以说我的计算机同时是 Web 客户机和 E-mail 客户机呢？答案：确实可以。

软件角度的服务器（Server）通常指一些安装了提供网络服务软件的计算机。比如，我们要提供网站服务就需要安装 Windows 2000 Server 或者 Windows Server 2003 服务器操作系统下的 IIS（Internet Information Server，Internet 信息服务器）软件，这里的 IIS 就是一种 Web 服务器软件，我们就称安装了 IIS 的计算机是一台 Web 服务器，依此类推。

问题	一台普通的 PC 可不可以安装像 IIS 这样的软件来提供网络服务呢？答案：当然可以，前提是只要你的 PC 能够为你的网络提供服务，而且服务的质量还能让你的老板和同事满意。

在本书的叙述中，除非特别声明，否则服务器和客户机都是从软件的角度来理解的。

1.3 网际互联模型

当网络刚开始出现时，典型情况下只能在同一制造商的计算机产品之间进行通信，例如只能实现整个的 DECnet 解决方案或 IBM 解决方案，而不能将两者结合在一起。20 世纪 70 年代后期，国际标准化组织（International Organization for Standardization，ISO）创建了开放系统互联（Open Systems Interconnection，OSI）参考模型，从而打破了这一壁垒。

OSI 模型的创建是为了帮助供应商根据协议来构建可互操作的网络设备和软件，以便不同供应商的网络设备能够互相协同工作。

OSI 模型是面向网络构建的最基本的层次结构模型，该模型采用分层的方法来实现数据和网络信息从一台计算机的应用程序，经过网络介质，传送到另一台计算机的应用程序。

在下面各节中，将讨论分层的方法，以及怎样采用分层的方法来排除互联网中的故障。

1.3.1 分层的方法

参考模型是一种概念上的蓝图，描述了通信是怎样进行的。它解决了实现有效通信所需要的所有过程，并将这些过程划分为逻辑上的层。层可以简单地理解成数据通信需要的步骤。当一个通信系统以这种层的方式进行设计时，就称为是分层的体系结构。

打个比方：将石家庄某厂大型机械设备搬到北京的某个房间中，需要哪些步骤呢？首先需要将设备拆卸，并对各个部件编号、打包，通过汽车运到石家庄火车站，通过火车运到北

京火车站，再通过市内交通工具运送到北京的房间，最后打开包装，将各个部件根据编号组装成设备。

在这种场景中，各个环节就隐喻了通信系统中的层。为了保证工作的顺利进行，每个环节都必须按标准交付给下一个环节，以保证下一个环节的正确运行。比如打包工人装箱必须能够符合汽车装载和运输，从汽车卸载下来的箱子，必须能够符合火车运输的标准。同时每个环节内部的变化不会影响其他环节，比如石家庄市建了许多立交桥给汽车运输提速，不影响打包工人的工作，也不影响火车的运输；火车提速了，不会影响室内的汽车运输或打包工人的工作。

一旦业务启动，各环节的人员就会做出与自己的部门有关的规划，他们需要制定实际的方案来实现所分配的任务。这些实际的方案，或者叫协议，需要被编辑成标准的操作规程手册，并加以严格执行。在手册中，每个不同的规程被赋予不同的解释，并伴有不同程度的重要性和实现性。如果你有一个合作伙伴或者成立了另一家公司，让他们遵守你的这些业务规程就是必不可少的（至少要相互兼容）。

类似地，软件开发者可以使用参考模型来理解计算机通信的过程，并看看在每一层中需要实现哪些类型的功能。如果他们正在为某一层开发协议，他们需要关心的只是这一层的功能，而不是任何其他层的功能。当然其他层的功能由其他层对应的协议来实现。

1.3.2 参考模型的优点

OSI 参考模型是层次化的，其主要意图，是允许不同供应商的网络产品能够在相应的层次上实现互操作。

采用 OSI 层次模型的优点如下。

- 将网络的通信过程划分为小一些、功能简单的部件，有助于各个部件的开发、设计和故障排除。
- 通过网络组件的标准化，允许多个供应商进行开发，比如定义以太网和广域网设备的接口标准和电压标准等。
- 通过定义在模型的每一层实现的功能，提高产业的标准化。
- 允许各种类型的网络硬件或软件相互通信，比如，思科公司的交换机和华为公司的交换机能够很好地连接通信；IE 浏览器和火狐狸浏览器都可以浏览网页等。
- 防止对某一层所做的改动影响到其他层，这样就有利于开发，比如你将组建局域网的设备由集线器替换成交换机，而你的路由器不需要更改；你的网站的改版，对网络设备也没影响等。

OSI 参考模型（OSI 规范）最重要的功能之一，是帮助不同类型的主机实现相互之间的数据传输，这意味着可以在一台 UNIX 主机和一台 PC 机或 Mac 机之间进行数据传输。尽管 OSI 模型不是物理意义上的模型，但它提供了一系列的指南，使应用程序开发者创建并实现在网络中运行的应用程序，它也为创建并实现联网标准、设备和网际互联方案提供了一个框架。

OSI 参考模型有 7 个不同的层，如图 1-5 所示。每层对应的功能，尤其是当前网络中普

遍应用的功能都包含在其中。



▲图 1-5　OSI 参考模型

- 应用层：提供用户接口，特指网络应用程序，能产生网络流量的应用程序，比如客户端的 QQ、MSN、IE 浏览器等，服务器端的 Web 服务、流媒体服务等。而 Windows XP 记事本程序和计算器程序由于不产生网络流量，所以它们不属于应用层。
- 表示层：表示数据，如采用二进制或 ASCII 码等；处理数据，如数据加密、数据压缩等。这一层常常是软件开发人员需要考虑的问题。比如 QQ 软件开发人员就要考虑用户的聊天记录在网络传输之前加密，防止有人使用捕包工具捕获用户数据，泄露信息；针对 QQ 视频聊天，开发人员就要考虑如何通过压缩数据节省网络带宽。
- 会话层：会话层的作用主要是建立、维护、管理应用程序之间的会话。比如流媒体服务器和每一个点播节目的客户端软件分别建立会话，服务器才能区分每个用户点播的节目和相应进度。
- 传输层：提供可靠或不可靠的传输，能够错误纠正，纠正失败能够重传。传输层的可靠传输负责建立端到端的连接，并负责数据在端到端连接上的传输。传输层通过端口号区分上层服务，并通过滑动窗口技术实现可靠传输、流量控制、拥塞控制以及通过三次握手建立连接。
- 网络层：为网络设备提供逻辑地址，根据数据包的逻辑地址选择最佳网络路径。负责数据从源端发送到目的端，负责数据传输的寻径和转发。
- 数据链路层：也经常被人们称为 MAC 层，它管理网络设备的物理地址，所以物理地址也被称作 MAC 地址。数据链路层将数据包封装为帧，使用 MAC 地址提供对介质的访问，执行差错检测，但不纠正。数据链路层向上提供对网络层的服务。
- 物理层：主要负责二进制数据比特流在设备之间的传输。物理层规定电压大小、线路速率、设备和电缆的接口标准。

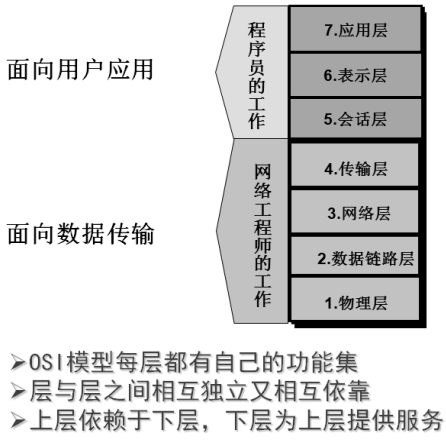
物理层关心的是以下一些内容。

- 接口和媒体的物理特性。
- 位的表示和传输速率。

- 位的同步。
- 物理拓扑：星状拓扑、环状拓扑、总线拓扑等。
- 传输模式：单工、半双工或全双工。

1.3.3 OSI 的分组

OSI 参考模型 7 个不同的层分为两个组，如图 1-6 所示。



▲图 1-6　OSI 模型分为两个组

上面 3 层为 OSI 的高层，主要面向用户应用，定义了终端系统中的应用程序将如何彼此通信，以及如何与用户通信。软件开发人员在开发应用程序时需要考虑 OSI 上面 3 层，不必要考虑数据通信方面的事情。

下面 4 层为 OSI 的底层，主要面向数据传输，定义了怎样进行端到端的数据传输。网络工程师的工作主要涉及 OSI 参考模型的下面 4 层。网络工程师负责把网络调通、优化后，就可以为多种应用程序提供网络通信。

1.4 理解 OSI 参考模型

以上对 OSI 参考模型的阐述，虽然是纯理论方面，但理解了之后，对以后的工作会有很大的帮助，下面讲几个例子来加深对 OSI 参考模型的理解。

1.4.1 实例：应用程序包含 IP 地址带来的麻烦

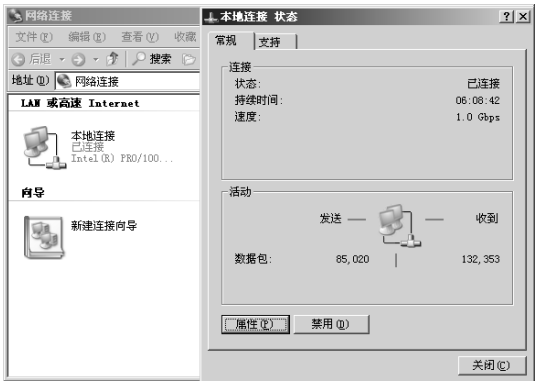
2000 年石家庄某医院的网络管理员打电话到我公司请求技术支持，问如何在不更改医院 IP 地址的情况下连接到市医保中心，市医保中心统一规划 IP 地址，要求医院重新规划 IP 地址。问题是现在医院的很多应用程序都是自己开发的，开发时客户端程序连接数据库服务器使用的都是 IP 地址，因此服务器的 IP 地址变化，会造成客户端连接数据库失败。

这就是应用层包含了网络层信息造成的麻烦，显然这是没有遵循 OSI 参考模型的理念。

如果是客户端程序使用域名连接数据库服务器，当服务器更改了 IP 地址以后，客户端可以根据域名使用 DNS 解析到新的数据库服务器的 IP 地址，这样应用层和网络层就没有关联了。

更改程序的工作量太大了，我公司最终选择通过给医院的计算机配置两个 IP 地址解决该问题，即医院计算机原来的 IP 地址保持不变，再根据市医保中心的地址规划，添加第二个 IP 地址。

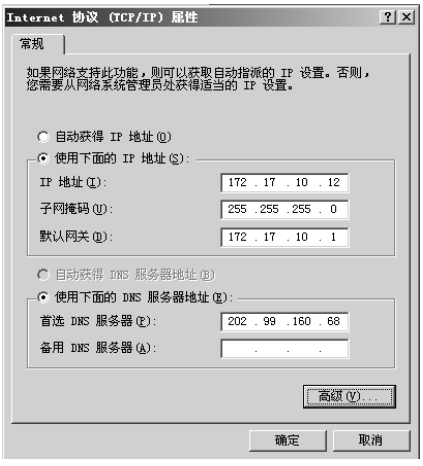
以下步骤可以为计算机添加多个 IP 地址，如图 1-7～图 1-10 所示。



▲图 1-7　打开“本地连接 状态”对话框



▲图 1-8　选择“Internet 协议（TCP/IP）”选项



▲图 1-9　设置 IP 地址



▲图 1-10　添加新的 IP 地址

1.4.2　OSI 参考模型与排错

OSI 参考模型中底层为其上层提供服务，因此排错也应该从底层到高层依次排错。

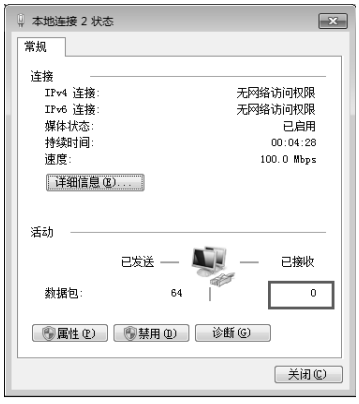
假若你是某公司的 IT 技术支持人员，某个员工打电话说不能打开网页了，该如何排错呢？

（1）物理层检查。首先查看网线是否连接正常。打开客户端的网络连接，如果出现红叉，如图 1-11 所示，则证明网线没有连接好，属于物理层故障。如果没有出现红叉，也不一定连接正常，双击，打开“本地连接 状态”对话框，查看“已发送”和“已接收”的数据包，其中任何一个为 0 都不能正常通信，如图 1-12 所示，可以检查网线

和网卡的接触是否有问题，用网钳重新压一压水晶头。



▲图 1-11　出现红叉

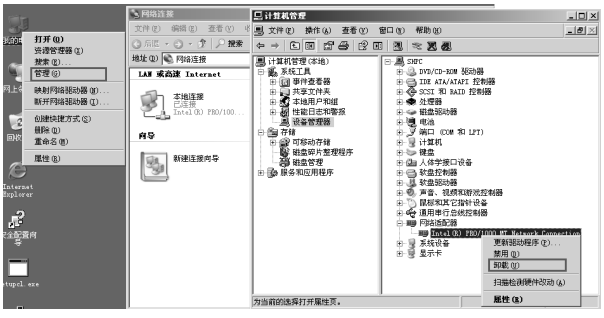


▲图 1-12　接收的包为 0

如果重新做了网线的水晶头，“已发送”或“已接收”的数据包仍为 0，则可以试试先卸载网卡驱动，再重新加载驱动，就能解决网卡驱动引起的网络故障。

鼠标右键单击“我的电脑”，在弹出的快捷菜单中选择“管理”命令，打开“设备管理器”界面，右击网卡，在弹出的快捷菜单中“卸载”命令。

在弹出的设备删除确认对话框中，单击“确定”按钮，如图 1-13 所示。



▲图 1-13　卸载网卡

可以看到删除了网卡驱动，本地连接也就没有了。

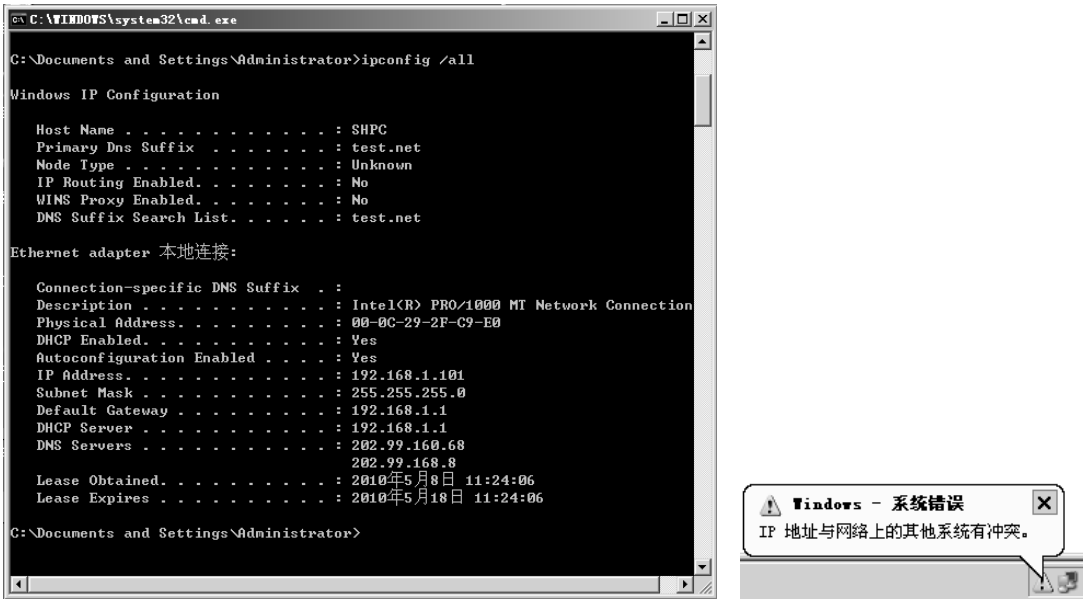
然后再次扫描检测硬件改动，就可以重新加载网卡驱动，本地连接又会出现，如图 1-14 所示。



▲图 1-14　重新扫描硬件

（2）数据链路层排错。ping 网关，如果时通时断，有可能是网络堵塞，也有可能是 MAC 地址冲突（我就碰到过 MAC 地址冲突的情况，使用 VMWare 克隆出一个操作系统，结果克隆的操作系统和现有的操作系统 MAC 地址冲突）；ping 网关不通，还要检查计算机连接的交换机的端口所属 VLAN 是否正确。

（3）网络层排错。首先看看 IP 地址是否配置正确，是否与其他 IP 地址有冲突，如果 IP 地址和网关配置错误也同样不能上网，如图 1-15 所示。



▲图 1-15　IP 地址错误

（4）表示层故障。比如我们打开的网页是乱码，就是表示层出现故障了。如图 1-16 所示，打开百度网页，能够正常显示页面内容。如图 1-17 所示，选择“查看”→“编码”→“其他”→“西里尔文”。如图 1-18 所示，IE 浏览器以西里尔文解释网页，则出现乱码。



▲图 1-16　表示层正常



▲图 1-17　更改 IE 编码



▲图 1-18　表示层出现错误

（5）应用层故障。查看 IE 的配置，如果 IE 安全级别设置得高，有些网页的功能则不能正常运行。如果设置了一个错误的代理服务器或安装了错误的 IE 插件也会造成网页打不开的现象。

1.4.3　通过建立的会话查看木马

通过查看可疑会话可以确认是否中了木马。

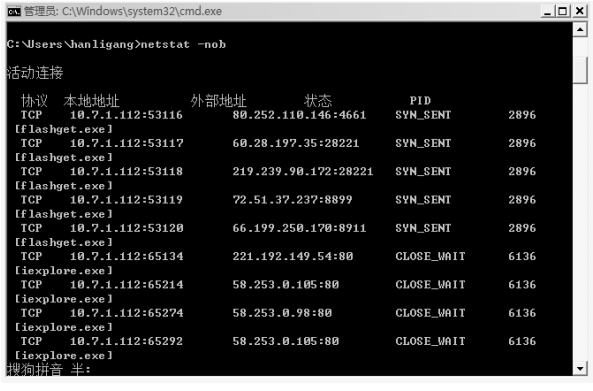
某单位的服务器最近出现异常，网络管理员感觉有人在操作他的服务器，于是他怀疑服务器中了木马。他想查看一下服务器是否中了木马，如何确认呢？

只要你的计算机中了木马，木马程序会自动运行，或者作为你的计算机上的一个服务，或者是开机就自动运行，然后就在后台偷偷地和远程的客户端连接。攻击者就可以看到哪些中了木马的计算机在运行，便可以操作中了木马的计算机。如果计算机中了木马，木马程序会自动和外网的客户端建立连接，我们可以通过查看计算机的对外连接来确认是否中了木马。

这位网管可以如下这样做。

首先需要登录计算机，但不访问任何网络资源，并且保证 Windows 没有在后台更新系统，杀毒软件也没有更新病毒库（因为这些活动也会建立会话，干扰你查找木马）。

如图 1-19 所示，运行 netstat –nob 查看有没有到 Internet 上的连接，可以看到源端口和目标端口，源地址和目标地址，以及建立会话的进程或程序。



▲图 1-19　通过 netstat –nob 查看连接

之后主要查看与外网地址连接的会话，如果有连接，那可能就是木马程序，即可看到进程号和该进程号对应的程序。

补充知识

还有一种方法查找木马，就是使用微软自带的系统配置工具 msconfig。木马一般会在操作的电脑上伪装成服务，或将自己放置在自动启动项，我们可以检查服务和自动启动项，查找可疑服务或程序。

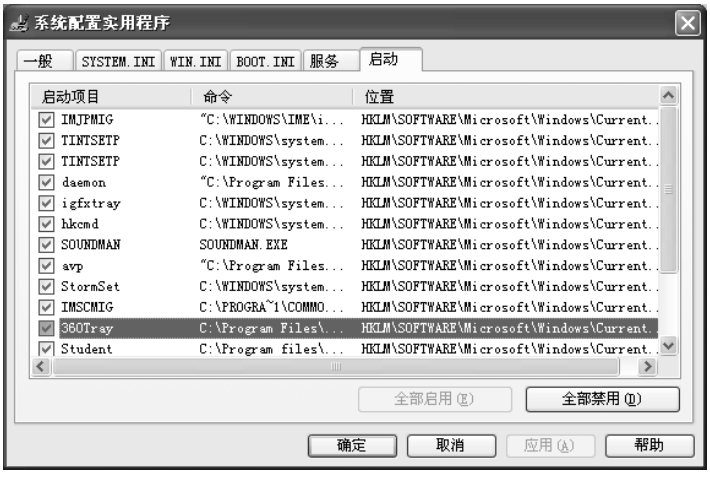
（1）选择“开始”→“运行”命令，打开“运行”对话框，输入 msconfig，单击“确定”按钮，打开“系统配置实用程序”对话框。

（2）如图 1-20 所示，切换到“服务”选项卡，选中“隐藏所有 Microsoft 服务”复选框，查看是否有可疑的服务。



▲图 1-20　隐藏所有 Microsoft 服务

（3）如图 1-21 所示，切换到“启动”选项卡，查看有没有可疑的自动启动项。如果有可疑的启动项，则将其禁用。



▲图 1-21　查看启动项

1.5 网络设备

要想组建网络，除了计算机和服务器之外，还需要网卡、网线、集线器、交换机和路由器设备。下面将介绍这些网络设备的相关知识。

1.5.1 网卡

计算机与外界局域网的连接是通过主机箱内插入一块网络接口板（或者是在笔记本电脑中插入一块 PCMCIA 卡）。网络接口板又称为通信适配器或网络适配器（adapter）或网络接口卡 NIC（Network Interface Card），但是现在更多的人愿意使用更为简单的名称——网卡，如图 1-22 所示。



▲图 1-22　网卡

网卡是工作在数据链路层的网络组件，是局域网中连接计算机和传输介质的接口，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存的功能等。

1．网卡的功能

随着集成度的不断提高，网卡上芯片的个数不断地减少，虽然现在各厂家生产的网卡种类繁多，但其功能大同小异，其主要功能有以下三个。

- 数据的封装与解封：发送时将上一层交来的数据加上首部和尾部，成为以太网的帧。接收时将以太网的帧剥去首部和尾部，然后送交上一层。
- 链路管理：主要是 CSMA/CD（Carrier Sense Multiple Access with Collision Detection，带冲突检测的载波侦听多路访问）协议的实现。
- 编码与译码：即曼彻斯特编码与译码。

2．网卡的传输速率

应根据服务器或工作站的带宽需求并结合物理传输介质所能提供的最大传输速率来选择网卡的传输速率。以以太网为例，可选择的速率就有 10Mb/s、10/100Mb/s、1000Mb/s，甚至 10Gb/s 等多种，但不是速率越高就越合适。例如，为连接在只具备 100Mb/s 传输速度的双绞线上的计算机配置 1000Mb/s 的网卡就是一种浪费，因为其最多只能实现 100Mb/s 的传输速率。

3．网卡的接口

网卡最终是要与网络进行连接的，所以也就必须有一个接口使网线通过它与其他计算机网络设备连接起来。不同的网络接口适用于不同的网络类型，目前常见的接口主要有以太网的 RJ-45 接口、细同轴电缆的 BNC 接口和粗同轴电缆的 AUI 接口、FDDI 接口、ATM 接口等。而且有的网卡为了适用于更广泛的应用环境，提供了两种或多种类型的接口，如有的网卡会同时提供 RJ-45、BNC 接口或 AUI 接口。

RJ-45 接口是最为常见的一种网卡，也是应用最广泛的一种接口类型网卡，这主要得益于双绞线以太网应用的普及。因为这种 RJ-45 接口类型的网卡就是应用于以双绞线为传输介质的以太网中，它的接口类似于常见的电话接口 RJ-11，但 RJ-45 是 8 芯线，而电话线的接口是 4 芯的，通常只接 2 芯线（ISDN 的电话线接 4 芯线）。在网卡上还自带两个状态指示灯，通过这两个指示灯颜色可初步判断网卡的工作状态。

4．MAC 地址

MAC（Media Access Control）地址，或称为物理地址、硬件地址，用来定义网络设备的位置。在 OSI 模型中，第三层网络层使用 IP 地址，第二层数据链路层使用 MAC 地址。因此一个主机会有一个 IP 地址，而每个网卡会有一个专属于它的 MAC 地址。

MAC 地址是烧录在 Network Interface Card（网卡，NIC）里的。MAC 地址是由 48 比特（6 字节）的十六进制的数字组成的。其中 0～23 位叫做组织唯一标志符（organizationally unique），是识别 LAN（局域网）结点的标识，24～47 位是由厂家自己分配。其中第 8 位是组播地址标志位。网卡的物理地址通常是由网卡生产厂家烧入网卡的 EPROM（一种闪存芯片，通常可以通过程序擦写），它存储的是传输数据时真正赖以标识发出数据的电脑和接收数据的主机地址。

也就是说，在网络底层的物理传输过程中，是通过物理地址来识别主机的，它一般是全球唯一的。比如，著名的以太网卡，其物理地址是 48 bit（比特位）的整数，如 44-45-53-54-00-00，以机器可读的方式存入主机接口中。以太网地址管理机构（除了管这个外还管别的）（IEEE）（IEEE：电气和电子工程师协会）将以太网地址，也就是 48 bit 的不同组合，分为若干独立的连续地址组，生产以太网网卡的厂家就购买其中一组，具体生产时，逐个将唯一地址赋予以太网卡。

形象地说，MAC 地址就如同我们身份证上的身份证号码，具有全球唯一性。

5．MAC 地址的应用

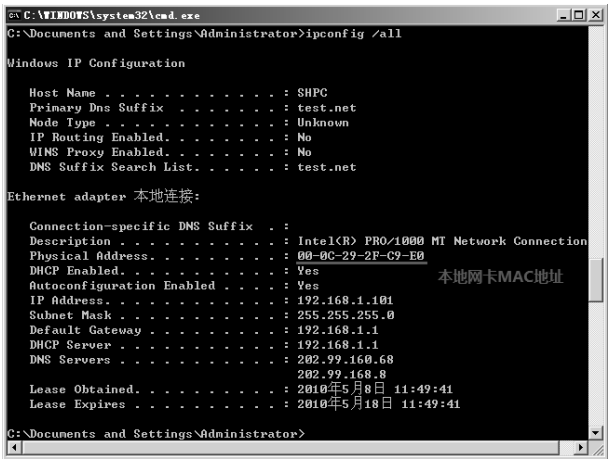
平日身份证的作用并不是很大，但是到了关键时刻，身份证就是用来证明你的身份的。比如你要去银行提取大额现金，这时就要用到身份证。那么 MAC 地址与 IP 地址绑定就如同我们在日常生活中的本人携带自己的身份证去做重要事情一样的道理。有的时候，我们为了防止 IP 地址被盗用，就通过简单的交换机端口绑定（端口的 MAC 表使用静态表项），可以在每个交换机端口只连接一台主机的情况下防止修改 MAC 地址的盗用，如果是三层设备还可以提供交换机端口/IP/MAC 三者的绑定，防止修改 MAC 的 IP 盗用。一般绑定 MAC 地址都是在交换机和路由器上配置的，是网管人员才能接触到的，对于一般电脑用户来说只要了解了绑定的作用就行了。比如你在校园网中把自己的笔记本电脑换到另外一个宿舍就无法上网了，这个就是因为 MAC 地址与 IP 地址（端口）绑定引起的。

6．查看和更改计算机的 MAC 地址

MAC 地址是绑定在网卡上的一个 12 位十六进制字符，它们在出厂的时候已经固化在网卡中，它是网卡在网络中的身份识别。有很多网络环境中都用到了 IP 地址和 MAC 地址绑定的情况。而 MAC 地址是先调入内存中后传输出去的，所以，我们可以通过修改其 MAC 地址来打破这些限制。

（1）如何获取本机的 MAC 地址？

在 Windows 2000/XP 中，依次选择“开始”→“运行”命令，在打开的对话框中输入“CMD”，单击“确定”按钮，在打开的命令窗口中输入“ipconfig /all”，回车。即可看到 MAC 地址，如图 1-23 所示。



▲图 1-23　查看 MAC 地址

（2）如何更改计算机的 MAC 地址？

① 如图 1-24 所示，打开“网络连接”窗口，右击“本地连接”，在弹出的快捷菜单中选择“属性”命令。



▲图 1-24　“本地连接 状态”对话框

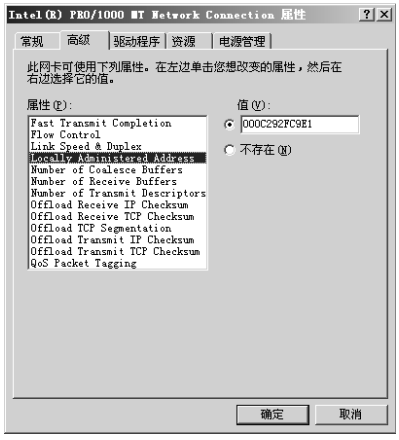
② 在出现的“本地连接 状态”对话框中，单击“属性”按钮。

③ 如图 1-25 所示，在出现的“本地连接 属性”对话框，单击“配置”按钮。

④ 如图 1-26 所示，在出现的属性对话框的“高级”选项卡的“属性”列表框中，选择 Locally Administered Address”，选中“值”文本框左侧的单选按钮，并在其中输入新的 MAC 地址。单击“确定”按钮。

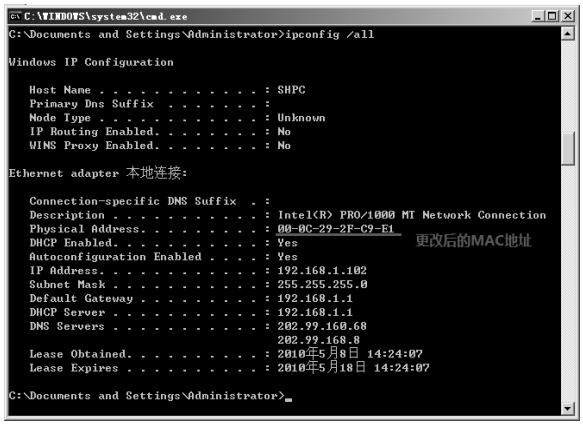


▲图 1-25　“本地连接 属性”对话框



▲图 1-26　输入新的 MAC 地址

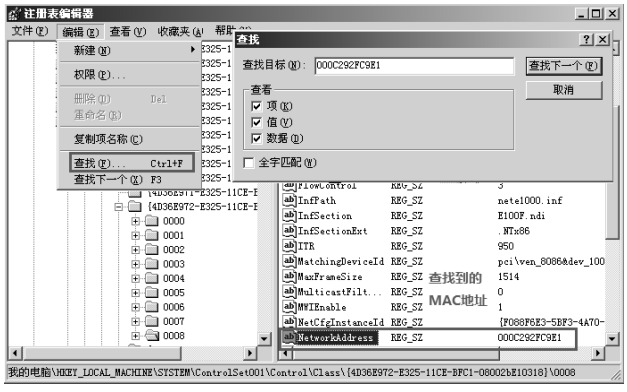
⑤ 如图 1-27 所示，在命令提示符下，输入 ipconfig /all 查看更改后的 MAC 地址。实际上网卡芯片的 MAC 地址并没有被改变。



▲图 1-27　查看更改后的结果

⑥ 更改后的 MAC 地址存储在计算机的注册表中，你可以搜索到。选择“开始”→“运行”命令，在打开的对话框中输入“regedit”，打开注册表编辑工具。

⑦ 如图 1-28 所示，选择“编辑”→“查找”命令，在出现的“查找”对话框中，输入 MAC 地址，就能搜索到上面更改的 MAC 地址。



▲图 1-28　在注册表中查看更改的结果

1.5.2 网线

以太网电缆的连接是一个重要的话题，尤其是在你打算参加 Cisco 考试的时候。可用的以太网电缆类型如下。

- 直通电缆
- 交叉电缆
- 反转电缆

下面将对这些电缆类型分别进行讨论。

1．直通电缆

直通线，又叫正线或标准线，两端采用 568B 做线标准，注意两端都是同样的线序且一一对应。

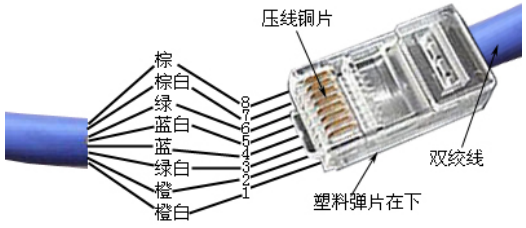
具体的线序制作方法如下。

双绞线夹线顺序是两边一致，统一都是：1—白橙、2—橙、3—白绿、4—蓝、5—白蓝、6—绿、7—白棕、8—棕，如图 1-29 所示。注意两端都是同样的线序且一一对应。这就是 100M 网线的做线标准，即 568B 标准，也就是我们平常所说的正线、标准线或直通线。

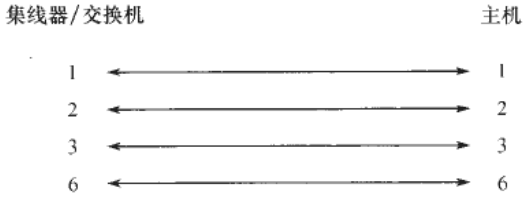
直通线应用最广泛，这种类型的以太网电缆用来实现下列连接。

- 主机到交换机或集线器
- 路由器到交换机或集线器

在直通电缆中，使用了 4 根电缆线来连接以太网设备。制作这种类型的电缆相对来说比较简单。图 1-30 所示是使用在直通以太网电缆中的 4 根电缆线。



▲图 1-29　568B 线序



▲图 1-30　直通线线序

> **注意**　只使用了 1、2、3 和 6 这些插脚引线。只需进行 1 到 1、2 到 2、3 到 3 和 6 到 6 的连接，就马上可以连网了。然而要记住，这些电缆只是以太网使用的，不能用于其他的网络，比如语音网络、令牌环和 ISDN 等。

2．交叉电缆

交叉线，又叫反线，线序按照一端 568A，一端 568B 的标准排列好线序，并用 RJ-45 水晶头夹好。

具体的线序制作方法如下。

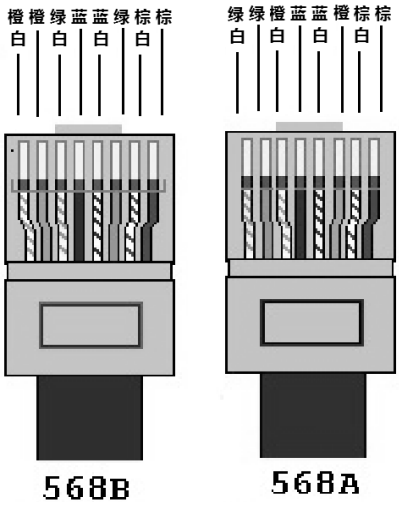
一端采用：1—白绿、2—绿、3—白橙、4—蓝、5—白蓝、6—橙、7—白棕、8—棕，即 568A 标准，如图 1-31 所示；另一端在这个基础上将这 8 根线中的 1 号和 3 号线，2 号和 6

号线互换一下位置，这时网线的线序就变成了 568B（即白橙，橙，白绿，蓝，白蓝，绿，白棕，棕的顺序）做线标准不变，这样交叉线就做好了，如图 1-31 所示。

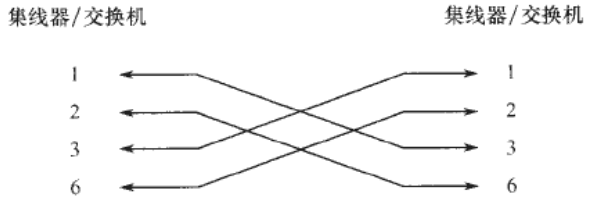
这种类型的以太网电缆用来实现下列连接。

- 交换机到交换机
- 集线器到集线器
- 主机到主机
- 集线器到交换机
- 路由器直连到主机

和在直通电缆中一样，这种电缆也使用 4 根同样的电缆线，但是要将不同的插脚引线连接起来。图 1-32 显示了这 4 根电缆线是怎样用在以太网交叉电缆中的。



▲图 1-31　568B 和 568A 的线序



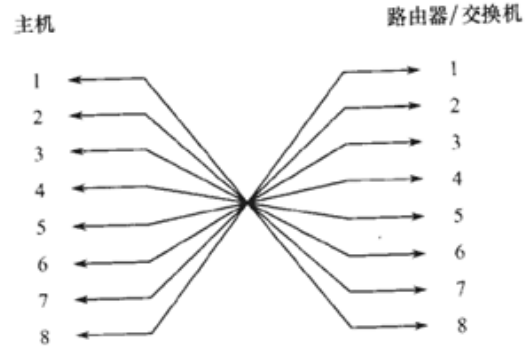
▲图 1-32　交叉线线序

3．反转电缆

尽管这种类型的电缆不是用来连接各种以太网部件的，但是你可以用它来实现从主机到路由器控制台串行通信（Console）端口的连接。

如果有一台 Cisco 路由器或交换机，就可以使用这种电缆将运行超级终端（HyperTerminal）的 PC 与 Cisco 硬件设备连接起来。在这种电缆中使用了 8 根电缆线来连接串行设备。图 1-33 显示了用在反转电缆中的 8 根电缆线。

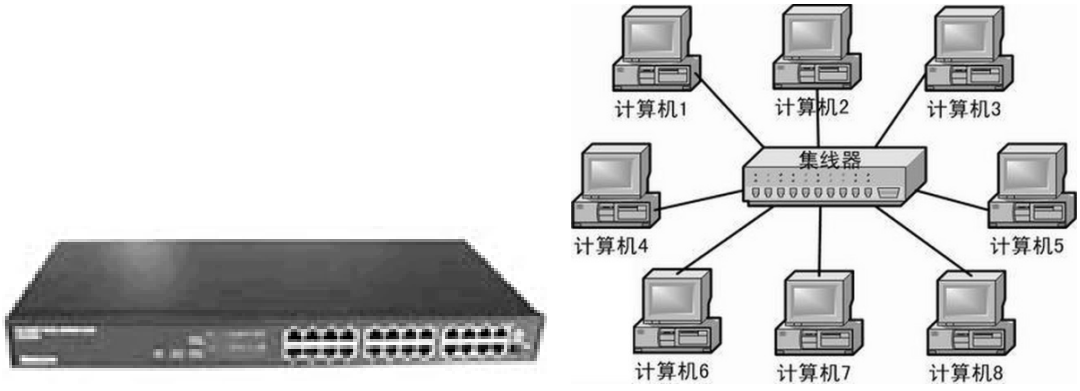
这些可能是最容易制作的电缆线了，因为你只需切断直通电缆线的一端，并将它反转过来连接即可（当然，要用另一个连接器）。



▲图 1-33　反转电缆线序

1.5.3 集线器

集线器的英文名称为“Hub”。“Hub”是“中心”的意思，集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有结点集中在以它为中心的结点上，如图 1-34 所示。



▲图 1-34　集线器配置图示

集线器工作于 OSI 参考模型的第一层，即物理层。它与网卡、网线等传输介质一样，属于局域网中的基础设备，采用 CSMA/CD 访问方式。

使用集线器的接入设备越多，冲突几率越大。

集线器使用 CSMA/CD 技术。

载波侦听多路访问/冲突检测 CSMA/CD 是一种介质访问的控制方法，当在同一个共享网络中的不同结点同时传送数据包时，不可避免地会产生冲突，而 CSMA/CD 机制就是用来解决这种冲突问题的。

1．CSMA/CD 的工作原理

当一个结点想在网络中发送数据时，它首先检查线路上是否有其他主机的信号在传送：如果有，说明其他主机在发送数据，自己则利用退避算法等一会再试图发送；如果线路上没有其他主机的信号，自己就将数据发送出去，同时，不停地监听线路，以确信其他主机没有发送数据，如果检测到有其他信号，自己就发送一个 JAM 阻塞信号，通知网段上的其他结点停止发送数据，这时，其他结点也必须采用退避算法等一会再试图发送。

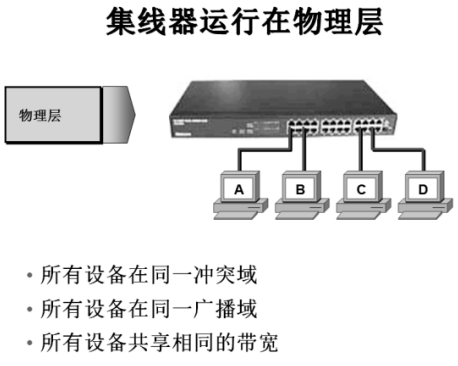
2．CSMA/CD 的重要特性

- 使用 CSMA/CD 协议的以太网不能进行全双工通信，而只能进行双向交替通信（半双工通信）。
- 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。
- 这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率。

集线器属于纯硬件网络底层设备，当网络中的 A 计算机和 B 计算机进行通信时，虽然数据帧有具体的源 MAC 地址和目标 MAC 地址，但是集线器不会针对目标 MAC 地址进行转发，而是将这个信号传递到所有的接口。也就是说，当它要向某结点发送数据时，不是直接将数据发送到目的结点，而是将数据包发送到与集线器相连的所有节结点，如图 1-35 所示。

这种广播发送数据方式有以下几方面不足。

- 用户数据包向所有结点发送，很可能带来数据通信的不安全因素，一些别有用心的人很容易就能非法截获他人的数据包。
- 由于所有数据包都是向所有结点同时发送，加上以上所介绍的共享带宽方式，就更可能造成网络堵塞的现象，越发降低了网络的执行效率。因此集线器连接的网为一个冲突域。
- 非双工传输，网络通信效率低。集线器的同一时刻每一个端口只能进行一个方向的数据通信，而不能像交换机那样进行双向双工传输，网络执行效率低，不能满足较大型网络通信的需求。



▲图 1-35　集线器运行在物理层

正因如此，尽管集线器技术也在不断改进，但实质上只是加入了一些交换机（switch）技术，发展到了今天的具有堆叠技术的堆叠式集线器，有的集线器还具有智能交换机功能。可以说集线器产品已在技术上向交换机技术进行了过渡，具备了一定的智能性和数据交换能力。但随着交换机价格的不断下降，仅有的价格优势已不再明显，集线器的市场越来越小，处于淘汰的边缘。尽管如此，集线器对于家庭或者小型企业来说，在经济上还是有一点诱惑力的，特别适合家庭中几台机器的网络或者中小型公司作为分支网络使用。

1.5.4　交换机

交换机（意为“开关”）是一种用于电信号转发的网络设备，它可以为接入交换机的任意两个网络结点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等，如图 1-36 所示。



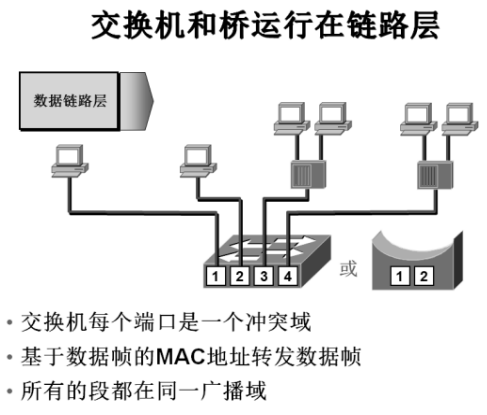
▲图 1-36　交换机图示

在计算机网络系统中，交换概念的提出改进了共享工作模式。我们之前介绍过的 Hub 集线器就是一种共享设备。Hub 本身不能识别目的地址，当同一局域网内的 A 主机给 B 主机传输数据时，数据包在以 Hub 为架构的网络上是以广播方式传输的，由每一台终端通过验证数据包头的地址信息来确定是否接收。也就是说，在这种工作方式下，同一时刻网络上只能传输一组数据帧的通信，如果发生碰撞还得重试。这种方式就是共享网络带宽。

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上，控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的 MAC（网卡的硬件地址）的 NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口，目的 MAC 若不存在则广播到所有的端口，接收端口回应后交换机会

“学习”新的地址，并把它添加到内部 MAC 地址表中。

使用交换机也可以把网络“分段”，通过对照 MAC 地址表，交换机只允许必要的网络流量通过。通过交换机的过滤和转发，可以有效地隔离广播风暴，减少误包和错包的出现，避免共享冲突，如图 1-37 所示。



▲图 1-37　交换机工作在链路层

交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。当结点 A 向结点 D 发送数据时，结点 B 可同时向结点 C 发送数据，而且这两个传输都享有网络的全部带宽，都有着自己的虚拟连接。假若这里使用的是 10Mb/s 的以太网交换机，那么该交换机这时的总流通量就等于 2×10Mb/s＝20Mb/s，而使用 10Mb/s 的共享式 Hub 时，一个 Hub 的总流通量也不会超出 10Mb/s。

总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据帧功能的网络设备。交换机可以“学习”MAC 地址，并将其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

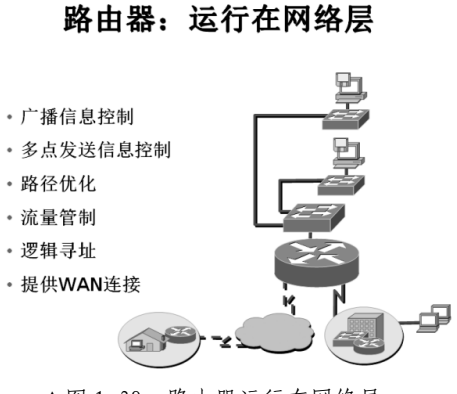
交换机和集线器相比有以下优点。

- 交换机的端口带宽独享。
- 交换机比集线器安全。
- 将目标 MAC 地址为 FF-FF-FF-FF-FF-FF 的数据帧发送到所有交换机端口（除了发送端口外），因此交换机连接的网是一个广播域。

因为交换机能够基于 MAC 地址转发数据，而 MAC 地址属于 OSI 参考模型的第二层地址，因此我们称交换机为二层设备。

1.5.5　路由器

路由器是连接因特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径、按前后顺序发送信号的设备。路由器的英文名是 Router，它是互联网的枢纽、“交通警察”。目前路由器已经广泛应用于各行各业，各种不同档次的产品已经成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的主力军，如图 1-38 所示。



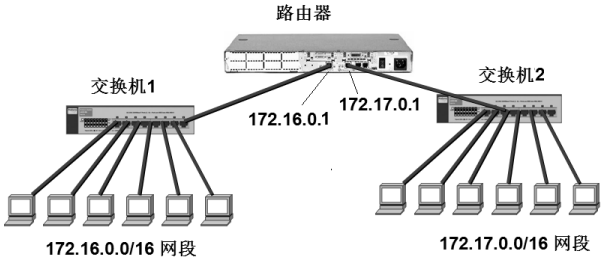
▲图 1-38　路由器运行在网络层

在路由过程中，信息至少会经过一个或多个中间结点。通常，人们会把路由和交换进行对比，

主要是因为在普通用户看来这两者所实现的功能是完全一样的。其实，路由和交换之间的主要区别就是交换机根据 MAC 地址转发数据帧，发生在 OSI 参考模型的第二层（数据链路层），而路由器基于网络层地址转发数据包，发生在 OSI 参考模型第三层，即网络层，因此我们说路由器为三层设备。

举例来说，大家都知道打电话分本地和长途，打长途电话需要拨区号，打本地电话则不需要拨区号。类似的来理解计算机之间的通信，交换机端口连接的计算机就相当于在同一个区的电话，负责在同一个区转发数据，即所连接的计算机的 IP 地址网络部分必须相同。路由器的接口连接不同的网段，负责在不同的网段转发数据包，相当于在不同区打长途电话。

如图 1-39 所示，交换机 1 连接的计算机都在 172.16.0.0/16 网段，交换机 2 连接的计算机都在 172.17.0.0/16 网段。路由器的两个以太网接口连接交换机 1 和交换机 2。连接交换机 1 的接口设置 IP 地址 172.16.0.1 作为 172.16.0.0/16 网段的网关，连接交换机 2 的接口设置 IP 地址 172.17.0.1 作为 172.17.0.0/16 网段的网关。网关就是到其他网段的出口，一般为路由器接口的 IP 地址，且该地址为该网段中第一个或最后一个可用的 IP 地址，这样可尽量避免计算机和网关的 IP 地址冲突。



▲图 1-39　使用路由器连网

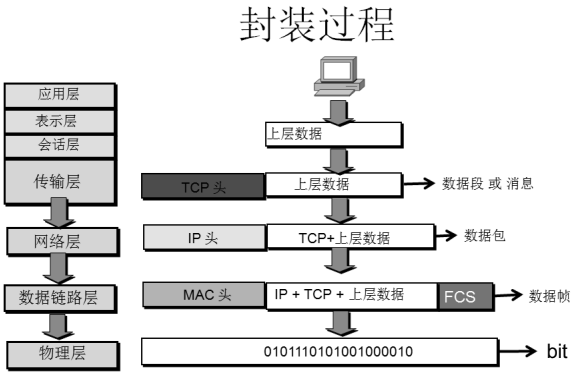
路由器是互联网的主要结点设备。路由器通过路由决定数据的转发，转发策略称为路由选择（routing），这也是路由器名称的由来（router，转发者）。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 国际互联网络 Internet 的主体脉络。也可以说，路由器构成了 Internet 的骨架，它的处理速度是网络通信的主要瓶颈之一，其可靠性则直接影响着网络互联的质量。因此，在园区网、地区网，乃至整个 Internet 的研究领域，路由器技术始终处于核心地位，其发展历程和方向成为整个 Internet 研究的一个缩影。

路由器的作用如下。

- 默认时，路由器将不会转发任何广播包或组播包。
- 在不同网段转发数据包，路由器使用 IP 地址，IP 地址在网络层的报头中，用来决定将包转发到的下一跳路由器。
- 路由器可以使用管理员创建的访问表来控制被允许进入或流出一个接口的包的安全性。
- 第三层设备 （这里是指路由器）可以提供虚拟 LAN（VLAN）之间的连接。
- 路由器可以为特定类型的网络流量提供服务质量（QoS）。

1.6 数据封装

数据要通过网络进行传输，要从高层一层一层地向下传送，如果一个主机要传送数据到别的主机，先把数据装到一个特殊的协议报头中，这个过程就叫封装（encapsulate/encapsulation），如图 1-40 所示。



▲图 1-40　数据封装

计算机在传数据之前需要将数据分段，在每段添加附加信息，称为封装。封装分为切片和加控制信息。

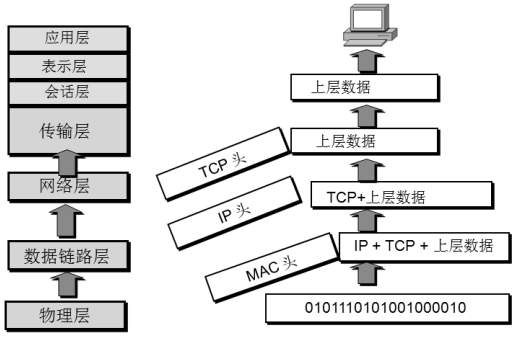
从事 IT 职业，我们经常会听到数据包、数据帧这样的名称。当数据在传输层添加上源端口和目标端口，我们称之为数据段或消息，可靠传输称为数据段，不可靠传输称为消息。在网络层会为数据段或消息添加目标地址和源地址，称为数据包。数据包在数据链路层添加了目标 MAC 地址、源 MAC 地址和帧校验序列（FCS），称为数据帧，如图 1-41 所示。



▲图 1-41　数据段/消息、数据包、数据帧的概念

在这里需要记住，数据包包括数据、端口和 IP 地址。数据帧包括数据、端口、IP 地址和 MAC 地址。

计算机在接收到数据帧后，需要去掉为了传输而添加的附加信息，这称为解封装，是上述封装操作的逆向过程，如图 1-42 所示。



▲图 1-42　解封装过程

1.7 传输模式

按照数据流的方向可分为三种传输模式：单工、半双工和全双工。

1．单工模式

单工（Simplex Communication）模式的数据传输是单向的。通信双方中，一方固定为发送端，一方则固定为接收端，信息只能沿一个方向传输。

单工模式一般用在只向一个方向传输数据的场合。例如，计算机与打印机之间的通信是单工模式，因为只有计算机向打印机传输数据，而没有向反方向的数据传输。还有在某些通信信道中，如单工无线发送、广播电台和收音机、电视台和电视之间的通信为单工模式。

2．半双工模式

半双工模式是指通信使用同一根传输线，既可以发送数据又可以接收数据，但不能同时进行发送和接收。数据传输允许数据在两个方向上传输，但是，在任何时刻只能由其中的一方发送数据，另一方接收数据。因此半双工模式既可以使用一根数据线，也可以使用两根数据线。它实际上是一种切换方向的单工通信，如同对讲机（步话机）一样。半双工通信中每端需有一个收发切换电子开关，通过切换来决定数据向哪个方向传输。因为有切换，所以会产生时间延迟，信息传输效率较低。

3．全双工模式

全双工模式是指数据通信允许数据同时在两个方向上传输。因此，全双工通信是两个单工通信方式的结合，它要求发送设备和接收设备都有独立的接收和发送能力，就和电话一样。在全双工模式中，每一端都有发送器和接收器，有两根传输线，可在交互式应用和远程监控系统中使用，信息传输效率较高。全双工以太网在原始的 802.3 Ethernet 中定义，它只使用一对电缆线，数字信号在线路上是双向传输的。当然，这与 IEEE 规范所讨论的全双工工作过程稍微有一点不同，但 Cisco 所说的通常是在以太网中所发生的事情。

1.7.1 半双工和全双工以太网

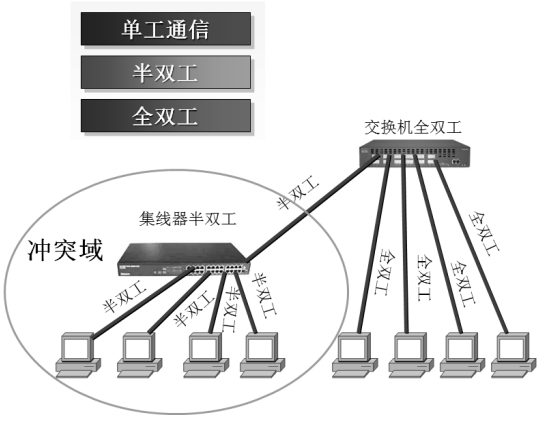
半双工以太网采用 CSMA/CD 协议，以防止产生冲突。如果产生冲突，就允许重传。如果使用集线器组建以太网，则必须工作在半双工模式，因为端站点必须能够检测到冲突。在 Cisco 看来，半双工以太网—典型的为 10BaseT，只有 30%～40%的效率。因为一个大的 10BaseT 网络通常最多只给出 3～4Mb/s 的带宽。

全双工以太网使用两对电缆线，而不像半双工模式那样使用一对电缆线。全双工模式在发送设备的发送方和接收设备的接收方之间采用点到点的连接，这就意味着在全双工数据传送方式下，可以得到更高的传输速率。由于发送数据和接收数据是在不同的电缆线上完成的，因此不会产生冲突。

全双工以太网之所以不会产生冲突，是因为它就像带多个入口的高速公路，而不是像半双工方式所提供的只有一条入口的路。全双工以太网能够在两个方向上提供 100%的效率。

比如，可以用运行在全双工方式下的 10Mb/s 以太网得到 20Mb/s 的传输速率，或者将 FastEthernet 的传输速率提高 200Mb/s，这是很了不起的。但是，这种速率有时被称为聚合速率，也就是说，你需要获得 100%的效率，就像生活中的事情一样，这不可能完全得到保证，如图 1-43 所示。

半双工和全双工以太网



▲图 1-43　半双工和全双工以太网

全双工以太网可以用于下列三种情况。

- 交换机到主机的连接。
- 交换机到交换机的连接。
- 使用交叉电缆的从主机到主机的连接。

最后，请记住下列重点。

- 在全双工模式下，不会有冲突域。
- 专用的交换机端口可用于全双工结点。
- 主机的网卡和交换机端口必须能够运行在全双工模式下。

1.7.2　设置网卡的双工模式

较新的计算机网卡双工模式或交换机的端口双工模式为自动协商方式。

自动协商的出现是为了保证新的全双工以太网兼容老的以太网。

自动协商的内容主要包括双工模式、运行速率以及流控等参数。

自动协商是建立在双绞线以太网的底层机制上的，它只对双绞线以太网有效。

假如 A 和 B 两端都支持自动协商，A 的工作速率有 10/100/1000Mb/s，B 的工作速率有 10/100Mb/s，那么它们协商的结果是 100Mb/s。这里很好理解，就是一个相与后取最大值的结果。

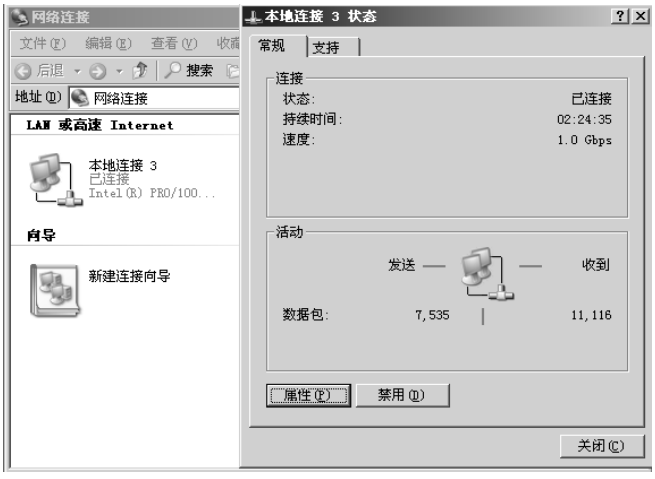
假如 A 和 B 两端中，A 支持自动协商，B 不支持自动协商，那么由于强行设定的站点不会告诉正在协商的站点自己的速率和单双工模式，自动协商的站点就必须自己决定合适的速率和单双工模式来匹配对端，这叫做平行检测。协商站点监听从对端过来的链路脉冲能够

辨别通信速率。10Mb/s、100Mb/s 和 1000Mb/s 以太网使用不同的信号模式，所以协商站点能识别对端的工作速率，然后达成一致。

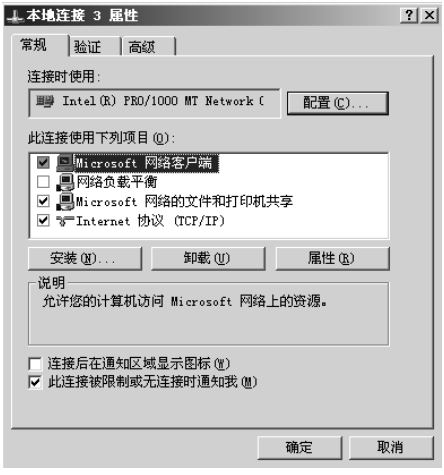
但假如 A 和 B 一个是半双工，一个是强行设定的站点。因为强行设定的站点不进行协商，协商站点无法知道强行设定站点工作在哪种双工模式下。根据 802.3 标准，它必须与强行站点使用相同的速率，但是工作在半双工模式下，不能检测到对端信息，则会产生全半双工不匹配的问题。

现在的电脑都是支持自动协商的，自动协商不再是问题了。

打开本地连接状态对话框，如图 1-44 所示，单击“属性”按钮，打开本地连接属性对话框，单击“配置”如图 1-45 所示。

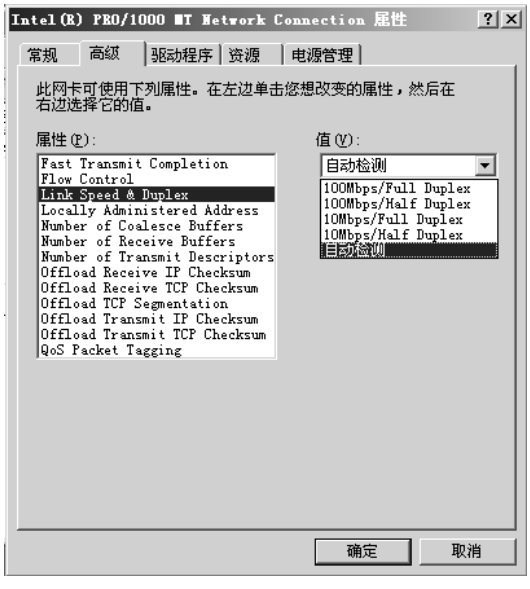


▲图 1-44　本地连接状态对话框



▲图 1-45　本地连接属性对话框

在“高级”选项卡的“属性”列表框中选中 Link Speed & Duplex 选项，可以看到默认是自动检测方式，如图 1-46 所示。你可以强制指定 100Mb/s 全双工、100Mb/s 半双工、10Mb/s 全双工和 10Mb/s 半双工。

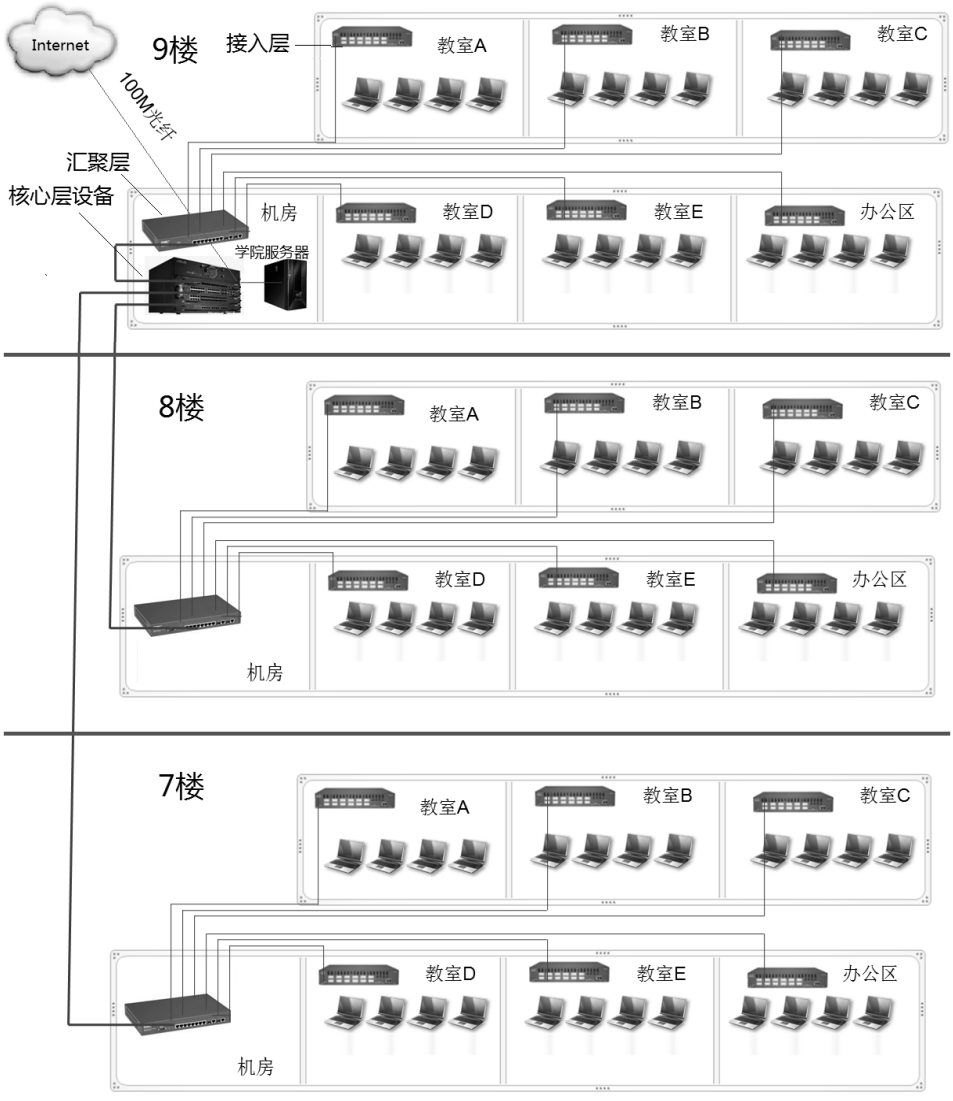


▲图 1-46　设置双工模式

1.8 Cisco 组网三层模型

现在以河北师范大学软件学院网络为例，介绍网络设备的部署位置和网络设备的层次。

河北师范大学软件学院位于田家炳楼的 7 楼、8 楼和 9 楼。在每间教室部署接入层交换机，每间教室的交换机为学生的笔记本提供网络接入。每层都有机房，在机房部署汇聚层交换机，连接教室中交换机，在 9 楼有核心层交换机，连接各个楼层的汇聚层交换机和学院的服务器，100Mb/s 光纤连接 Internet，如图 1-47 所示。



▲图 1-47　软件学院网络示意图

Cisco 的层次模型可以用来帮助设计、实现和维护可扩展、可靠、性能价格比高的层次化互联网络。Cisco 定义了三个层次，每一层都有特定的功能。

下面是这三个层次和它们的典型功能。

- 接入层，Layer 2 Switching，最终用户被许可接入网络的点。

- 汇聚层，Layer 3 Switching，接入层设备的汇聚点。
- 核心层，Layer 2/Layer 3 Switching，高速交换背板，不进行任何过滤，因为会影响转发速度。

1.8.1 核心层

从字面意义上看，核心层（Core Layer）就是网络的核心。它位于顶层，负责可靠而迅速地传输大量的数据流。网络核心层的唯一意图是，尽可能快地交换数据流。跨核心层传输的数据流对大多数用户来说是公共的。然而要记住，用户数据是在汇聚层进行处理的，如果需要的话，汇聚层会将请求转发到核心层。

如果核心层出了故障，就会影响到每一位用户。因此，核心层的容错就成了一个问题。核心层很可能流过大量的数据，因此，速度和延迟在这里是分别考虑的。给出了核心层的功能，现在我们就可以考虑一些设计问题了。让我们从不应该做的事情谈起。

- 不要做任何影响到通信流量的事。其中包括使用访问列表、在 VLAN 之间进行路由选择以及进行包过滤。
- 不要在这里支持工作组接入。
- 当互联网络扩展时（比如添加了路由器），应避免扩充核心层。如果核心层的性能成了问题，就应当升级而不是扩充。

现在，我们来看看在设计核心层时应当做的一些事情，包括下面这些。

- 在设计核心层时一定要实现高可靠性，考虑采用对速率和冗余都有利的数据链路层技术，比如 FDDI、带有冗余链路的快速以太网，甚至 ATM。
- 在设计时一定要时刻想着传输速率，核心层的延迟应当非常小。
- 选择收敛时间短的路由协议。如果路由表收敛慢的话，快速的和有冗余的数据链路连接就没有意义了。

1.8.2 汇聚层

汇聚层（Distribution Layer）有时也称为工作组层，它是接入层和核心层之间的通信点。汇聚层的主要功能是提供路由、过滤和 WAN 接入，如果需要的话，它还决定数据包可以如何对核心层进行访问。汇聚层必须决定用最快的方式来处理网络服务请求。比如，一个文件请求如何被转发到服务器。在汇聚层决定了最佳路径后，它就将请求转发到核心层，由核心层将请求快速传送到正确的服务中。

汇聚层是实现网络策略的地方，在这里，可以在所定义的网络操作中试验其灵活性。在汇聚层上，有一些通用的操作，包括下面这些。

- 路由。
- 工具的实现，比如访问表、包过滤和排序。
- 网络安全和网络策略的实现，包括地址翻译和防火墙。

- 重新分配路由协议，包括静态路由。
- 在 VLAN 之间进行路由，以及其他工作组所支持的功能。
- 定义广播域和组播域。

在汇聚层应当避免做的事情有限，主要是不能使用专门属于其他层的功能。

1.8.3 接入层

接入层（Access Layer）控制用户和工作组对互联网络资源的访问。接入层有时也称为桌面层。大多数用户所需要的网络资源将在本地获得，由分配层处理远程服务的数据流。下面是接入层的一些功能。

- 连续的访问控制和策略（对汇聚层的延续）。
- 创建分隔的冲突域（分段）。
- 到汇聚层的工作组连通性。

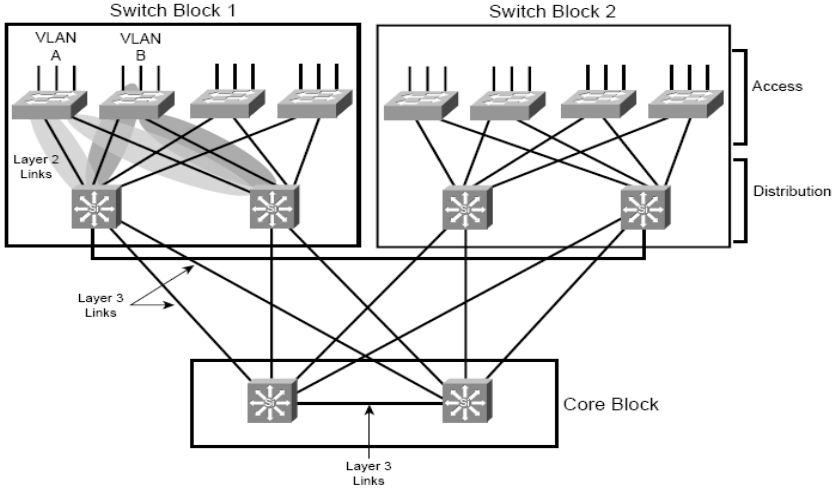
在接入层经常采用诸如 DDR 和以太网交换这样的技术，这里采用静态路由（而不是动态路由协议）。

大家应该想得到，三个不同的层次并不意味着需要三台不同的路由器，也许要少一些，也许要多一些。记住，这只是一种逻辑上的分层方法。

1.8.4 高可用网络设计

思科的层次模型可以帮助您设计、实施和维持一个可扩展、可靠、最具成本效益的分层互联网。

如果企业的网络非常重要（比如医院的网络）。为了避免汇聚层和核心层设备故障造成网络故障，可以设计成双核心层和双汇聚层，如图 1-48 所示。



▲图 1-48　双核心层和双汇聚层网络

1.9 习 题

1. 开放系统互联参考模型简称_____。
2. OSI 参考模型分为_____层，分别是_____、_____、_____、_____、_____、_____ 和_____。
3. 物理层传送数据的单位是_____，数据链路层传送数据的单位是_____，传输层传送数据的单位是_____。
4. 在 OSI 参考模型中，七层协议中的__（1）__利用通信子网提供的服务实现两个用户进程之间端到端的通信。在这个模型中，如果 A 用户需要通过网络向 B 用户传送数据，则首先将数据送入应用层，在该层为它附加控制信息后送入表示层；在表示层对数据进行必要的变换并加头标后送入会话层；在会话层加头标送入传输层；在传输层将数据分解为__（2）__后送至网络层；在网络层将数据封装成__（3）__后送至数据链路层；在数据链路层将数据加上头标和尾标封装成__（4）__后发送到物理层；在物理层数据以__（5）__形式发送到物理线路。B 用户所在的系统接收到数据后，层层剥去控制信息，把原数据传送给 B 用户。

（1）A．网络层　　B．传输层　　C．会话层　　D．表示层
（2）A．数据包　　B．数据流　　C．数据段　　D．报文分组
（3）A．数据段　　B．数据包　　C．路由信息　　D．报文分组
（4）A．数据段　　B．数据包　　C．数据帧　　D．报文分组
（5）A．比特流　　B．数据帧　　C．数据段　　D．报文分组

5. 路由器是一种常用的网络互连设备，它工作在 OSI 的__（1）__上，在网络中它能够根据网络通信的情况__（2）__，并识别__（3）__。相互分离的网络经路由器互连后__（4）__。通常并不是所有的协议都能够通过路由器，如__（5）__在网络中就不能被路由。

（1）A．物理层　　B．数据链路层
　　C．网络层　　D．传输层
（2）A．动态选择路由　　B．控制数据流量
　　C．调节数据传输率　　D．改变路由结构
（3）A．MAC 地址
　　B．网络地址
　　C．MAC 地址和网络地址
　　D．MAC 地址和网络地址的共同逻辑地址
（4）A．形成了一个更大的物理网络
　　B．仍然还是原来的网络
　　C．形成了一个逻辑上单一的网络
　　D．成为若干个互联的子网

（5）A．NetBEUl　　B．Apple Talk
　　C．IPX　　D．IP

6. 属于物理层的互连设备是_____。
　A．中继器　　B．网桥
　C．交换机　　D．路由器

7. 在 OSI 参考模型中，物理层的功能是__（1）__，网络层的服务访问点也称为__（2）__，通常分为__（3）__两部分。
（1）A．建立和释放连接　　B. 透明地传输比特流
　　C．在物理实体间传送数据帧　　D. 发送和接受用户数据
（2）A．用户地址　　B. 网络地址
　　C. 端口地址　　D. 网卡地址
（3）A．网络号和端口号　　B. 网络号和主机地址
　　C．超网号和子网号　　D. 超网号和端口地址

8. 在 OSI 参考模型中，_____实现数据压缩功能。
　A. 应用层　　B. 表示层
　C. 会话层　　D. 网络层

9. 按照网络分级设计模型，通常把网络设计分为三层，即核心层、汇聚层和接入层。以下关于分级网络的描述中，不正确的是_____。
　A. 核心层承担访问控制列表检查功能
　B. 汇聚层实现网络的访问策略控制
　C. 工作组服务器放置在接入层
　D. 在接入层可以使用集线器代替交换机

10. 下列_____设备可以隔离 ARP 广播帧。
　A. 路由器　　B. 网桥
　C. 以太网交换机　　D. 集线器

11. 在 OSI 参考模型中，实现端到端的应答、分组排序和流量控制功能的协议层是_____。
　A．数据链路层　　B．网络层
　C．传输层　　D．会话层

12. 在层次化园区网络设计中，_____是接入层的功能。
　A．高速数据传输　　B．VLAN 路由
　C．广播域的定义　　D．MAC 地址过滤

习题答案

1. OSI
2. OSI 参考模型分为 7 层，分别是应用层、表示层、会话层、传输层、网络层、数据链路层、物理层。
3. 物理层传送数据的单位是比特，数据链路层传送数据的单位是数据帧，传输层传送数据的单位是数据段。
4. （1）C、（2）C、（3）B、（4）C、（5）A
5. （1）C、（2）A、（3）B、（4）A、（5）A
6. A
7. （1）B、（2）B、（3）B
8. B
9. A
10. A
11. C
12. C